Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.
The blank line after that segment is not intended; final line printed: "Automating the protection of sensitive data is important because even people with the"

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes.

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These

numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information*

Security report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP

technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is

still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the

same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human

errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of

a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some

sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and

only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions

best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

swift number BOSHCNSHHZA

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.

swiftroutingnumber BKCHUS33CTX

Automating the protection of sensitive data is important because even people with the best of intentions make mistakes. The 2008 edition of CompTIA's *Trends in Information Security* report estimated that 30 percent of serious data breaches are caused by human errors, another 30 percent are caused by a hacker taking advantage of a human error, and only 40 percent are caused by a hacker actively overcoming flaws in technology. These numbers are quite a bit different than they were five years ago. The 2003 edition of the same report estimated that only 8 percent of serious data breaches did not involve some sort of human error.

People are getting better at protecting sensitive data, but they still not very good at it. It is still the case that most serious data breaches are caused by a failure of people instead of a failure of technology. Because of this, automating the process of protecting data will give

much better results that just relying on error-prone people, and that is exactly where DLP technology promises to be able to make a difference.