[8 practices for business data security](https://www.red-gate.com/blog/audit-and-compliance/8-practices-business-data-security" \o "8 practices for business data security)

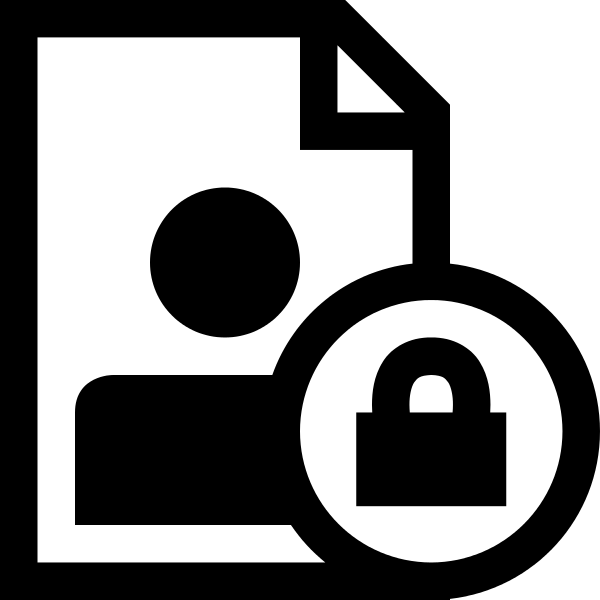
[Sophie Ross](https://www.red-gate.com/blog/author/sophie-ross" \o "Posts by Sophie Ross)

17 August 2018

FROM: <https://www.red-gate.com/blog/audit-and-compliance/8-practices-business-data-security>

Guest post

This is a guest post from Sophie Ross. Sophie is a marketing specialist at [**Security Gladiators**](https://securitygladiators.com/). A writer by day and a reader by night, she specializes in tech and cybersecurity. When she isn't behind the screen, Sophie can be found playing with her dog.

These days, everything from buying clothes to banking is done online, and this is all thanks to technology. The shift of transactional and record-keeping systems from physical to virtual has led to an unprecedented amount of problems, the most troublesome of which are around security.

Implementing data security in any business is an ongoing process, however, because of the volatile nature of cyber threats. Hackers and viruses form only a portion of the threats to your business’s data and, to have full coverage and a fluidly responsive [**information security system**](https://www.red-gate.com/simple-talk/sysadmin/data-protection-and-privacy/information-security-in-practice/), it is essential to adopt the following best practices.

1. Use multiple layers of security

One of the most costly mistakes an organization can make when it comes to protecting its data is failing to provide full coverage against all possible threats.

Several companies adopt strong anti-virus and anti-malware security solutions but omit the inclusion of disaster recovery services. Often, these companies are caught flat-footed when their physical data systems are the targets of threats they had not prepared for.

Another blind spot that many businesses succumb to is [**internal security threats**](https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company). Sometimes, an organization can be compromised from the inside. This occurs when too many employees have access to a company’s sensitive data, even when it is not in direct relation to their duties at the company. A sound data security system should cover against all threats—internal and external—by using techniques like encryption and data masking.

2. Involve the entire staff

Educating staff on what to do to [**prevent data loss and theft**](https://www.pcmag.com/article/348925/6-ways-to-train-your-employees-to-prevent-cyberattacks) is the first step to ensuring a robust security system. That’s because knowing what to do in the event of an emergency situation can be the key to business continuity, particularly when customer data is at stake.

Most malware attacks target low-level staff, so leaving them unprepared is leaving the business open to several vectors of cyberattacks.

3. Deploy preventative measures

Your security system should include both preventative and actionable measures in the event of an emergency. To be able to preemptively defend against attacks from different vectors, it may be necessary to get in the mind of the attacker.

This involves directly looking for weaknesses in your system, but will largely entail judging your system’s biggest vulnerabilities and whether they’ll hold off any malicious entities.

4. Have a dedicated security team

Having a dedicated security team that constantly monitors the state of data security and actively responds to threats could be the difference between saving and losing your data.

A security team will be the first to respond to reports of any malicious activity within the system and could save your company the cost of hiring security experts even for minor events.

5. Minimize employee access to sensitive levels

Only allow your employees access to the levels of information they need to accomplish their duties. This can be achieved in many cases with standard access controls, but sometimes employees require copies of production databases for use in development, testing and business analytics. Here, sensitive data should be masked, rather than replaced with anonymous data, in order to retain its referential integrity and distribution characteristics.

To further minimize the risk of employee fraud, consider splitting responsibilities between employees to prevent leaving too much authority focused on a few select individuals. A sound security system should also have the ability to log employee activities to discourage fraud and information theft.

6. Secure data input and output hardware

Your employees’ laptops are some of the weakest links in your security system. Often, [**phishing attacks**](https://www.wsj.com/articles/the-anatomy-of-a-phishing-attack-1527645601) target the personal devices used by the people working at the company.

An efficient security system should provide additional security for data endpoints such as laptops, tablets, and smartphones. State-of-the-art software should not only prevent against cyber attacks but also provide remote security features that allow the company to lock and locate stolen devices.

7. Keep sensitive data encrypted

Data is often at its most vulnerable when in transit, which is why you should keep your sensitive data perpetually encrypted. This makes it less prone to interceptions when moving it from physical storage to cloud servers, or from the server to server.

Encrypted data can still be intercepted, but it is useless to attackers who cannot decipher the data without the appropriate decryption protocol.

**8. Routinely test your security systems**

A security system that’s never been tested is potentially as good as no security. You have to know the strengths and weaknesses of your own system before pitting it against third-party entities which will stop at nothing to get what they want. It may be appropriate to [**bring in a white-hat hacker**](https://www.information-age.com/go-hack-yourself-what-white-hat-hacking-and-why-are-businesses-turning-it-123460624/) periodically to test if your systems are good enough to withstand an attack in a real-life situation.

Summary

Data security is a major concern for businesses of all sizes. Data breaches can cost businesses [**hundreds of thousands of dollars or more**](https://securityintelligence.com/news/cost-of-average-enterprise-data-breach-surpasses-1-million/) in losses and damages, not to mention significant damage to brand reputation.

While security is crucial, it remains poorly implemented by some businesses who think their data is not at risk. In reality, data security doesn’t just revolve around keeping hackers away from your customers’ credentials. Sensitive data subject to privacy regulations should always be protected internally, and data loss in the event of a fire, an on-site robbery or the corruption of storage devices should be guarded against.