16-CNBC-Lessons from Target

Tech

As the risk of data breaches are on the rise, so are the number of attacks and financial impact on American businesses.

For executives at companies experiencing data breaches, the consequences can be even more dire. It can cost managers their jobs.

Five months after Target ‘s holiday data breach, the retailer’s former chairman and chief executive Gregg Steinhafel stepped down from his more than $23 million-a-year position. While Steinhafel also faced criticism for Target’s Canadian expansion, the massive breach—which included leaked credit and debit card information for millions of customers—likely played a role, according to analysts. *[Deny]*

“Gregg [Steinhafel] led the response to Target’s 2013 data breach. He held himself personally accountable and pledged that Target would emerge a better company,” the company said in a May 5 statement. *[Rebuild]*

Craig Carpenter, a chief strategist at cybersecurity company AccessData, said the information security community believes the resignation will “help raise information security to a C-level [corporate] issue.”

A Target customer prepares to sign a credit card slip.

Getty Images

Business managers are paying closer attention to information security because the costs of data leaks only are expanding.

Since last year, data breaches on average have risen 15 percent to $3.5 million, according to a new study by IBM and the Ponemon Institute, a researcher on data protection and information security.

The costly damage to a business includes expenses related to seeking experts' help, the actual company investigation and any loss of customers. Part of the 15 percent increase can be attributed to more customer records being stolen.

Here's what corporate executives and business managers need to learn about data breaches.

Cybersecurity is everyone's issue.

After data breaches, the person who usually takes blame is the chief information security officer or the chief information officer, Carpenter said. In the case of Target, the chief information officer resigned in March before the chief executive's departure.

The acknowledgement that all senior managers are responsible for data security is part of the challenge.

A study by cybersecurity firm Stroz Friedberg found that just 45 percent of senior management acknowledged they are responsible for protecting against cyberattacks.

Shawn Henry—cybersecurity expert and a former executive assistant director of the FBI—said companies need to acknowledge every employee is responsible for cybersecurity, not just the tech guys. "Technology is a piece of the solution but it's not the sole solution," said Henry, now president of cybersecurity company CrowdStrike Services.

Detect breaches and mitigate effects

VIDEO2:0502:05