How IT Security Training Can Mitigate the Risk of a Data Breach

THE CHALLENGE

In this case, the company affected by a data breach was not one of our customers, but it is still a valuable lesson we would like to share. In 2013, as the holiday shopping season approached, security staff of the major retailer Target ignored the alerts generated by its malware software. On November 30, 2013, the hackers deployed their custom-made code, triggering a FireEye alert that indicated unfamiliar malware. Target's Symantec anti-virus system apparently found suspicious activity around the same time. FireEye software could have even automatically deleted the malware, but the function was turned off.

An estimated 110 million customer records were exposed. The cost to the company ranged from $400 to 450 million, with a major dent in the brand's reputation. The lesson here is that there's a limit to what security systems can do. Training in how to use those solutions is critical. At some point, people must take the reins and investigate alerts, review events, research solutions and configure systems. The most sophisticated security solutions can't operate without trained human intervention, as the Target data breach demonstrates.

THE SOLUTION

If Target had been our client following its security breach, we would have advised three steps:

1. **Educate management to get buy-in**
   A commitment to IT security needs to come from the top. If upper management doesn't see IT security as a priority in their risk-management process, then they won't budget for it. Continuing to keep management in the loop as to how the security investment is paying off is critical.

2. **Educate the end-users**
   An annual security awareness class is the minimum requirement for end-user education. Many companies have a program, but a 2013 Ponemon/Symantec Cost of Data Breach Study shows that 62% of breaches are caused by employee and system errors.

3 Educate the IT staff

How much security training does the IT staff receive? Do they know the security vulnerabilities in their systems and the best practices for securing virtual systems, databases and network devices? There are many online and classroom classes to educate IT staff, with some focusing on securing types of systems (Windows, UNIX), virtual systems, databases and networking/firewalls. Companies like Kaizen Approach can provide consultation and customized training.

THE RESULTS

Target hired a Chief Information Security Officer (CISO) six months later to mitigate the risk of a future attack. It surprised many in the cybersecurity industry that a large corporation would not have a full-time CISO on staff. Kaizen Approach believes that a CISO is essential to the cybersecurity of every organization, no matter the size. In response, we offer what we call the Virtual CISO. This service offers cost-effective and high-quality security experience to companies that may not have or need a full-time CISO. We take our customers through the three steps above, among many other functions depending on their needs.

Learn more here about our Virtual CISO service or contact us to discuss your challenges. You can also view our full presentation related to the Target breach here.

CONTACT US