TOLMAN & WIKER INSURANCE SERVICES, LLC
INNOVATIVE RISK ADVICE SINCE 1923™
VENTURA | LOS ANGELES | SALINAS | SANTA MARIA | BAKERSFIELD

## Five Valuable Takeaways from Recent Cyber Breaches

March, 2014

Property Casualty 360

The hits just keep coming. In the last few months alone we've learned of at least five major data breaches at five large companies, from retail to hospitality, arts and crafts to foodservice. The silver lining, if we're pragmatic enough to look for it, is that there are valuable lessons we can take from each of these breaches.

**1. Communicate quickly and carefully.** Initial word of the Target breach, which potentially compromised more than 100 million credit and debit cards, didn't come from the company. Instead, a highly respected security blogger is the one who broke the news. Target finally released its own public response, but customers were further confused by e-mails that didn't appear to be legitimate (the company used an unfamiliar domain to send the messages, giving the impression it was a phishing e-mail that should be deleted).

Customers don't want to learn they've been a victim of fraud second-hand and they definitely don't want to see a company they entrusted with sensitive information fumbling something as simple as an e-mail domain. That kind of reputational damage is difficult to overcome. Target's move to offer a 10% discount may have been a sign it was feeling a bottom-line-affecting backlash.

**2. Hackers aren't the only concern.** In the Coca-Cola breach, we saw the theft of more than 50 laptops containing sensitive data for more than 70,000 people. The thief? A former employee. The timeline? Several years. That's right, IT equipment was leaving the premises over a period of years, and no one was the wiser.

The most secure perimeter in the world doesn't do much if the threat is already inside the walls. Companies must formulate comprehensive data protection programs that include defense of external connections as well as internal physical access.

**3. Develop (and enforce) policies for all levels of the network.** It's startling how many of these large exposure cases are discovered by external organizations. In the White Lodging breach, where the hotel and restaurant management company experienced the exposure of payment card data that may have gone on for nearly 9 months before the security hole was closed, it was an astute banking industry that uncovered the fraud. Regular network monitoring and security audits should catch most suspicious activity long before it reaches this sort of scale.

In addition, some of these breaches call into question how well companies are separating their most sensitive data from other, less confidential information. Effective security protocols work in layers, affording the highest degree of protection to data that truly needs it. In addition, systems and databases containing sensitive data should have hardened defenses to deflect attacks that originate in other parts of the network.

**4. Institute controls for vendor access.** It appears the Target breach was perpetrated using credentials stolen from an HVAC contractor who provided services to the retail giant. In today's increasingly inter-connected world, businesses have more privileged access into others' systems than ever before.

Target's breach teaches us that network authorization must be carefully controlled. External partners with access should have strict protocols in place to manage how their credentials are used within their own organization, to monitor usage patterns, and to limit or shut down access at the first sign of suspicious behavior.

**5. Make the right response tools available.** Breaches aren't created equal, and some will expose different types of information than others. Retail breaches often involve payment card data but not personal information such as social security numbers. In those instances, the typical knee-jerk reaction is to provide affected customers with free credit monitoring, as Target and others have done.

Credit monitoring typically doesn't catch fraudulent use of existing accounts, which is where victims in these types of breaches are most likely to be impacted first. Instead, customers should be encouraged to monitor their existing accounts for suspicious activity. In the Coca-Cola breach, on the other hand, credit monitoring is precisely the right tool to offer victims. Because social security numbers may have been compromised, careful oversight of credit files could help to stop potential fraud.



**Forward this article to a colleague**

Address To | Recipient Name

Subject

Message

Send | Reset