Are you a Target?

By Kevin Baughn

You no doubt have heard about the massive credit card data theft involving nearly 100 million credit card numbers that happened to Target during the crucial holiday shopping season of 2013. Could something similar happen to you? Is your sensitive data protected as well as it should be? Do you understand the potential ramifications to your reputation and bottom line if sensitive information is lost or stolen?

Here is a brief summary of what occurred at Target: Outside hackers obtained access to Target’s internal networks by using an access code Target provided to a third party HVAC (air conditioning) company who needed limited access to Target’s systems. The hackers then infected Target’s point of sale system and allowed them to collect unencrypted credit card data directly from the card swipe pads in most of their stores.

Target is a huge retailer with revenues around $73 billion in 2013. You might expect a company of this size would have state of the art data security and would be able to detect and thwart such attacks. And they do. In fact, Target recently reported that their cutting edge outside security monitoring agency detected the attack shortly after it began but took no action because it was just one of hundreds of attack warnings Target sees daily. This is an excellent example to illustrate that no matter how secure you (or your IT department) think you are there is still risk. And this applies to all different types of companies large and small.

How do you protect yourself? In Target’s case it was mostly credit card numbers stolen. Card numbers were not encrypted at the swipe pad. Encryption didn’t occur until after being transmitted to Target’s central credit card data repository, and this was the weak link exploited by the hackers. Protecting yourself from data breaches means eliminating as many weak links as you can.

Here are a few things to focus on:

- **Less is better:** Store the minimum amount of sensitive information you need in order to do business. Sensitive information includes personal information about your customers and employees such as Social Security numbers, credit card numbers, addresses, protected health information, driver’s license numbers, and secret or proprietary business information about third party businesses. The less information you keep the less risk you have that it can be lost or stolen.

- **PCI compliance:** If you are accepting credit/debit cards for payment, be sure you are PCI-compliant. PCI stands for “payment card industry” and provides data security standards for the protection of credit card data. There are PCI self-assessments for smaller merchants and third party assessments for larger ones. More information can be found here: [https://www.pcisecuritystandards.org](https://www.pcisecuritystandards.org). For smaller merchants who outsource their entire card processing to a third party (and you store no card numbers yourself), be sure you ask your processor if they, and the POS equipment they provide you, are fully PCI-compliant.

- **Encrypt:** For the information you do need to keep, be sure you keep it in encrypted format. This is often something dismissed by companies because it costs money to implement. But when you consider what the costs would be if your data was stolen, suddenly encryption looks cheap in comparison. If encrypting data in transit, at rest, and on mobile devices is prohibitive, at least focus on mobile devices such as whole disk encryption for...
laptops and ensure that if you electronically transmit data to third parties, you do so in encrypted format.

- **Limit access:** Most data losses/thefts happen as a result of negligence or intentional actions by employees who have authorized access to your network. Be sure you limit employee access to sensitive information on a need to know basis and educate them on how sensitive data should be handled. When an employee leaves, disable their network access codes immediately.

- **Purchase insurance:** It was leaked publicly that Target had $100 million in privacy liability insurance in place. With the amount of lost data involved and the number of lawsuits already filed against them on behalf of consumers and by credit card issuing banks, the $100 million may easily be exhausted. This insurance coverage generally also covers the costs to notify the persons affected to and pay for public relations/crisis management expenses as well as the costs of offering credit monitoring or other remediation services. Once you have focused on addressing your weak links, you might consider buying insurance to protect you in the event something happens despite your best efforts. Insurance provides coverage for costs incurred by you to comply with notification laws (including legal fees to determine a response), forensic costs to investigate what happened, and defense and payments of fines due to governmental actions against you after a privacy breach (such as the FTC, OCR, etc.). It also provides defense and payment of damages if there are any third party claims against you. Another great benefit of having insurance is that your carrier will offer guidance through what is a labyrinth of varying state and federal laws so that you can comply with your legal obligations and protect your reputation as much as possible.

Insurance should not be considered a “catch all” that will solve all potential problems. In Target’s case, the $100 million in insurance may be a drop in the bucket compared to their lost revenues and profit resulting from a damaged reputation/loss of trust. Target’s fourth quarter revenues were down 5.3% from the prior year, and profits down 46%, and none of that is insurable. Target will recover in time, but you should ask yourself if your business would be able to withstand an event where your customers lose faith in you.

Safehold Special Risk offers comprehensive and broad privacy liability insurance supported by Certain Underwriters at Lloyd’s of London. We have products available for both small and large organizations, with customizable coverage options. For more information regarding this topic or Safehold Special Risk, please contact Helen Richards at 720-963-6540 or helen.richards@safehold.com.