Courtesy of
Berends Hendricks Stuit Insurance Agency

CYBERRISKS&LIABILITIES_

Lessons From the Target Data Breach

In late 2013, Target, the large American retailer, was the victim of a massive data breach that affected as many as 110 million customers. Cyber attackers installed malicious software on point-of-sale devices at Target stores and were able to steal the financial information of 40 million customers and the personal information of 70 million.

From lawsuits and fines to the costs of offering free credit monitoring and hiring a computer forensics investigator, this breach is massive not only in terms of how many customers it's affected, but also in terms of how much of a financial hit Target will take. Target's cyber insurance policy will cover some of the monetary damages, but the damage to its reputation and customer loyalty will not be easy to recover.

No business is immune to a data breach—not even a nationwide retailer like Target. But your business can survive a data breach if you are prepared to handle it and if you have the proper cyber liability coverage to help you successfully respond to it.

Be Prepared With a Data Breach Response Policy
Target experienced a decrease in sales immediately following customer notification of the breach. Customers didn't feel safe shopping there with a debit or credit card, and many customers' potentially compromised cards were cancelled by banks. Target tried to remedy this by offering a discount and free credit monitoring, but it may have been too late for some customers.

A data breach can directly affect your relationship with your customers or clients. They may not feel safe doing business with you anymore, and you must be prepared to prevent that.

One way to proactively protect your business is to create a data breach response policy—it will serve as your roadmap during a data breach. It will help employees work together to minimize the damage your business could suffer, and also ensure that your customers get consistent responses. Your data breach policy should address:

- What to do when you first learn of the breach
- What information to include in your risk assessment
- Whether notification is required, and who must be notified
- Developing a plan to control risks

What's My First Move After a Breach Happens?
On Dec. 19, Target disclosed that it had experienced a data breach from Nov. 27 to Dec. 15. Customers wondered why Target had waited four days to inform them, but the company was most likely using that time to assess the damage and risks and prepare its response.

If you experience a data breach, the first thing to do is find out as many facts as you can about the breach so you can notify customers. Determine when and how the breach occurred, what information was obtained and how many individuals were affected.

Then assess the risks you face by determining:

- The sensitivity of the information
- The number of individuals affected
- The likelihood the information is usable or could cause harm
- The likelihood the information was intentionally targeted (increases chance for fraudulent use)
- The strength and effectiveness of your cyber security

bhs
Berends|Hendricks|Stuit

By fully analyzing the data breach, the information you give to your customers or clients is as accurate as possible and will hopefully ease their worries. And if the information is coming directly from you, your customers may feel confident that you have control of the situation.

Solid Customer Notification Is Key
Customers criticized Target for not responding to the data breach right away. When Target finally did say something about it, customers saw the response as unapologetic and too formal.

The way a company responds to a data breach can build or damage the trust and loyalty of customers. Tailor the response to your audience. Be understanding of how your customers or clients feel, because you probably feel the same way—you are both victims of the breach.

Improve Your Cyber Security Protocols
Soon after the breach, Target announced to customers that it had invested in internal processes and systems to reduce the chances of a data breach happening again. It also said it was working with a computer forensics firm to investigate the breach in hopes that it could determine the cause and repair it.

Every company has data to protect, whether it's client or customer data, employee data or other company information. Data breaches can be devastating if you lack effective security protocols. Encrypting your sensitive data, using role-based monitoring to detect suspicious insider activity and adopting the National Security Administration's "two-person rule" are actions you can take to strengthen your protection.

Regularly review your security protocols to ensure your data is adequately protected. Keep in mind that as technology evolves, cyber criminals evolve, too, and their attacks become even more sophisticated and targeted.

Possible Impact on Your Company's Leadership
Five months after disclosing its data breach, Target faced big changes in its executive leadership—CEO Gregg Steinhafel left the company after 35 years, seven of which he had served as CEO. Steinhafel's departure came shortly after Target's Chief Information Officer, Beth Jacob, stepped down from her position.

After the breach, Target struggled to regain customer loyalty, which negatively impacted sales as well as the price of its shares. Target's board was plagued with questions about whether it had responded quickly enough to the breach, further damaging the company's reputation.

Target's story shows that the aftereffects of a data breach impact more than just your cyber security measures. Your company's leadership may change, either voluntarily or out of necessity, so you must be ready to react.

Protect Your Business With Cyber Liability Coverage
Notifying customers, setting up a call center dedicated to breach-related calls and providing free credit monitoring are a few ways Target responded to the data breach. These actions are costly, but fortunately for business owners, cyber liability coverage can help defray some of those costs.

Every company is a potential target for cyber criminals. Don't think of a data breach as a possibility but as an expectation, and always be prepared to respond. Contact Berends Hendricks Stuit Insurance Agency today for more information on data breaches and to learn about the cyber liability coverage options for your business.