RISK INSIGHTS Retail

Marshall & Sterling INSURANCE

Protect Your Online Retail Network

With the increasing popularity of smartphones and tablets, access to online shopping websites is only a fingertip away for most consumers. As a result, the online retail industry is an increasingly attractive target for major cyber attacks. The results—including tarnished reputations, lost sales and costly lawsuits—can be devastating.

This happened to Zappos, a large online shoe and apparel store owned by Amazon. Cyber criminals broke into Zappos' internal network and stole personal information from 24 million customers, including names, addresses and the last four digits of credit card numbers. Zappos attempted damage control by informing their customers about the incident and advising them to change their passwords, but much of the damage was already done.

As an online retail business, your success is dependent on the health and security of your biggest tool—your network. In order to protect your network and keep your online business profitable, it is critical that you understand the risks you face.

Hackers and Hacktivists

Do you think hackers only target big brand retail websites that can gain them national attention? Think again. In reality, data thieves are simply looking for the path of least resistance, and have begun to realize that small to medium size online retailers make easier targets because they generally lack IT departments and the high-level security software that big retailers have. Despite the increasing number of large and high publicized cyber attacks, 85 percent of small business owners believe their company is safe from cyber attacks.

A cyber attack could knock a small to midsize online retailer offline for days, causing them to lose sales, customers and their reputation. Worse yet, a single data breach could even force some small retailers out of business. Visa, Inc. estimates that 95 percent of the credit card data breaches reported to them happened with their smallest business customers.

Not all hackers are after customers' credit card numbers. "Hacktivists" attack computers or computer networks as a means of political protest. They're not just targeting government websites, though. In April 2011, hacktivist group Anonymous attacked the Sony® website in hopes of gaining attention about recent legislation called the Stop Online Piracy Act (SOPA). They gained attention, and Sony's website was offline for hours.

The online retail industry is an increasingly attractive target for major cyber attacks. The results—including tarnished reputations, lost sales and costly lawsuits—can be devastating.

What is a DDoS Attack?

Hackers can attack online retailers in a number of ways, one of which is a distributed denial of service (DDoS) attack. DDoS is a type of cyber attack in which a hacker floods your retail website with traffic and overwhelms your server to the point that your legitimate customers are unable to access your site. DDoS attacks can last a

few hours to a few days; meanwhile, your company loses out on business and may incur the cost of bringing in an IT specialist to investigate and stop the attack.

Can You Prevent a DDoS Attack?

Industry experts report that DDoS attacks have risen 30 percent in recent years. This could cause a huge loss for online retailers, especially if the attack occurs on Cyber Monday or during the busy holiday shopping season. Although many times DDoS attacks occur on larger brand online retailers, no retailer is immune. Small and midsize companies that rely on larger e-commerce providers or payment processing companies could be affected if those larger companies come under attack.

With DDoS attacks, you'll usually never find the source of the attack. Instead, focus on procedures to carry out once an attack happens, including communicating the incident to customers.

Mitigate the DDoS Risk

To mitigate some risks that DDoS attacks pose, it is important to understand your Web hosting environment. Some examples of Web hosting include the following:

- Shared hosting, in which multiple websites share a single server. This is the most common and economical option for small companies, as the host likely already has a DDoS response plan in place.
- Cloud hosting, a newer platform where the hosting is decentralized and users are only charged for the services they use, not a flat fee.
- In-house hosting, in which a company, such as a larger online retailer, hosts its own site and assumes all of the responsibility for DDoS attacks.

Many small and midsize online retailers use shared hosting because they don't have IT departments and the capabilities to host their own sites. When selecting a Web hosting service, consider the following:

- Does the hosting company cater only to e-commerce clients or to a variety of clients? The behavior of other users on the server could impact the performance of your website.
- How many websites are packed on a single server?
- What type of DDoS response plan does the host have in case of an attack on the network?

Data Breaches

Hackers love to steal credit card data, and online retail websites have plenty of data available. With the increased use of wireless networks, data theft can occur more easily. Cyber threats include fraud, worms and viruses.

Most websites use secure socket layers (SSL), which are supposed to guarantee that log in, password and credit card information is safe during a customer's online shopping. SSL relies on special electronic certificates issued to a secure website, but each Internet browser validates the certificates in a different way. Keep in mind that SSL is not immune from hacking, and beware of fake certificates.

Mitigate Data Breaches

Are you providing your customers with a secure online shopping experience? Consider the following:

- Comply with the Payment Card Industry-Data Security Standard (PCI-DSS). Merchants who don't can get fined by credit card companies.
- Purchase as much security as you can afford. Consider how much lost customer data or lost customers would cost your company.
- Maintain continuous vigilance of your site and know your real customers.

- Have firewall segmentation between wireless networks and point-of-sale networks, or in front of any network that comes in contact with credit card information.
- If you suffer a data breach, communicate this to your customers.

Cyber security is a serious concern for online retailers of all sizes. We are here to help. Contact Marshall & Sterling, Inc. to learn about our risk management resources and insurance solutions, such as Internet/Media Liability, Security and Privacy Liability and Identity Theft insurance today.