RISK INSIGHTS Retail

INSURANCE BROKERS Robison Challenging Convention

Protect Your Online Retail Network

Online retailers have been experiencing huge growth in recent years, making them increasingly attractive targets for major cyberattacks. Understanding cybersecurity risks and protecting your network is crucial to keeping your online company in business.

Hackers and Hacktivists

Do you think hackers only target big brand retail websites? Think again. Hackers have begun to realise that small to medium sized online retailers make easier targets because they generally lack Information Technology (IT) departments and the high-level security software that big retailers have.

A cyberattack could knock a small- to medium-sized online retailer offline for days, causing it to lose sales, customers and its reputation. Worse yet, a single data breach could even force some small retailers out of business. Visa, Inc. estimates that 95 per cent of the credit card data breaches reported to them happened with their smallest business customers.

What is a DDoS Attack?

Hackers can attack online retailers in a number of ways, one of which is a DDoS attack. DDoS, or distributed denial of service, is a type of cyberattack 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 anywhere from 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?

Although DDoS attacks often occur on larger brand online retailers, no retailer is immune. Small and medium sized companies that rely on larger e-commerce providers or payment processing companies could be affected if those larger companies come under attack.

> A cyberattack can knock a small to medium sized online retailer offline for days.

Mitigate the DDoS Risk

To mitigate some of the DDoS risk, it is important to understand your Web hosting environment. Some examples of Web hosting include:

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

Many small and medium sized online retailers use shared hosting because they don't have the capability to host their own site. When selecting a Web hosting service, consider the following:

- Does the hosting company only cater to e-commerce clients, or to a variety of clients? The behaviour 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 a cyberattack to the network?

Data Breaches

Hackers love to steal credit card data, and online retail websites have plenty of that. With the increased use of wireless networks, data theft can occur more easily. Cyberthreats 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 are safe during a customer's online shopping. SSL relies on special electronic certificates issued to a secure website, but each 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:

- Purchase as much security as you can afford. Consider how much a single breach 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.

Cybersecurity is a serious concern for online retailers of all sizes. We are here to help. Contact Robison & Co Ltd to learn about our risk management resources and insurance solutions for cyber liability.