Cyber Risks & Liabilities

May/June 2019

Cyber Attacks Increasing for Canadian Organizations

In the last year, an alarming majority of Canadian establishments reported falling victim to multiple cyber attacks, according to a recent report by Carbon Black. These breaches are not only incredibly costly to the organizations and encouraging to their perpetrators, but are in many cases preventable through basic diligence of cyber security maintenance.

Increased Frequency and Complexity

The report found that a staggering 83 per cent of surveyed organizations reported suffering a cyber security breach in the last year, with 22 per cent reporting five or more breaches in that time. This high number of breaches per organization is further supported by the 76 per cent of Canadian organizations that reported an increase in cyber attacks in the last year. Furthermore, 25 per cent of organizations reported that the number of attacks had increased by half since the previous year.

However, cyber attacks on Canadian businesses haven't only grown in frequency, but have also grown in complexity, with 81 per cent of surveyed organizations reporting that the attacks they had experienced in the last year were more complex than those of previous years.

Who Is Affected

While no organization is completely immune to cyber attacks, the survey showed that 83 per cent of larger organizations (over 5,000 employees) reported increased attacks, while only 65 per cent of small businesses (under 250 employees) reported an increase in cyber attacks.

Understanding and Preparing for the Threat

The dark economy is currently valued at more than US$1 trillion. Of those surveyed, only 10 per cent of respondents correctly identified that statistic, demonstrating the lack of understanding that can ultimately lead to exploitable exposures.

Of the different types of cyber attacks, malware is the most prolific, with 30 per cent of surveyed respondents reporting that malware was the most commonly encountered attack. However, phishing was the cause of successful breaches at 20 per cent of organizations, and "watering hole" tactics were reported to be the most effective and destructive of cyber attacks by 30 per cent of respondents.

Outdated security technology and processes accounted for 20 per cent of breaches, indicating that routine maintenance and updating of cyber security technology and policies could greatly benefit many organizations. In fact, 86 per cent of respondents reported that threat-hunting strengthened their defence.

In response to the destructive nature and increasing prevalence of threats, 85 per cent of surveyed organizations reported plans to increase their cyber defence budgets.

Megson FitzPatrick Insurance Services
3561 Shelbourne Street
www.megsonfitzpatrick.com

Megson FitzPatrick INSURANCE SERVICES

Cyber Criminals: Who Are They and What Motivates Them?

While we commonly think of cyber criminals as singular individuals bunkered up in a basement, the truth is that attackers are often much more sophisticated. Let's examine the most common threats to your business:

- **Insiders—**While your employees are some of your best assets, they can also be one of your greatest threats. In some cases, well-meaning employees accidently put confidential information at risk through careless cyber security practices. Other times, disgruntled employees will vandalize assets or steal proprietary data to get back at your organization.
- **Organized crime—**Organized cyber criminals are primarily interested in money. These groups often seek personally identifiable information like social insurance numbers, health records, credit card details and banking information. They then hold this information hostage through ransomware or sell it outright on the dark web to turn a profit.
- **Hacktivists—**Hacktivists operate with a political agenda, often carrying out high-profile attacks to distribute propaganda or damage organizations they disagree with. Hacktivists typically fall under the category of cyber vandalism and look to damage reputations or steal incriminating information.
- **Government-sponsored groups—**These cyber criminals are well-funded and are typically motivated by political, economic, technical or military agendas. Government-sponsored attacks are often very sophisticated, and these groups target highly sensitive and competitive proprietary data.

Cyber Security Tools for Your Business

If your organization falls victim to a cyber attack, your valuable digital assets could be compromised. There are several precautions you can take to limit the possibility for criminals to break into your organization's systems and wreak havoc.

Firewalls—Firewalls are software that control the incoming and outgoing network traffic on a computer system and determine what should and should not be allowed through. Most computer operating systems now come with a pre-installed firewall for basic but reliable security, however it may be beneficial to compare alternatives in order to find a firewall that fits your organization's unique needs.

Routers—Routers are hardware that keep unwanted traffic out of a computer system. They differ from firewalls in that they are stand-alone devices that must be bought separately–they are not included in an operating system. Look for routers with advanced security protocols.

Antivirus programs—As their name implies, antivirus programs are designed to catch and eliminate or quarantine viruses before they can harm a computer system. Antivirus programs run in the background to ensure your computer is protected at all times. While they are updated frequently, they may not catch the newest viruses that are floating around.

Cloud—A cloud is a data centre available to many users that is hosted in a centralized, often off-site server that is accessible via an internet connection. Clouds are especially beneficial for cyber security simply because it is much easier to secure a single cloud structure than to secure hundreds of individual employee computers.

Penetration testing—In order to test how your organization would fare against a possible cyber attack in a safe environment, regularly perform penetration testing. Penetration testing consists of hiring cyber security professionals to attempt to perform cyber attacks on your organization for the purpose of identifying vulnerabilities in your cyber security and recommending solutions to prevent such attacks from being successful in the future.

Education—Every company, no matter its size, should educate employees on the dangers of computer intrusions and how to prevent them. For example, make sure your employees know not to open, click on or download anything inside emails from untrusted sources, and to disregard emails with subject lines and attachments that seem bogus or too good to be true. Employees with an intimate knowledge of the company's computer network should also be alerted of the potential consequences of hacking into the system.

Review your risks and coverage options—A computer intrusion could cripple your company, costing you thousands or millions of dollars in lost sales and/or damages. Contact Megson FitzPatrick Insurance Services today. We have the tools necessary to ensure you have the proper coverage to protect your company against losses from computer intrusions.