CYBERRISKS+LIABILITIES

September/October 2018

IN THIS ISSUE

CCV INSURANCE & FINANCIAL
a division of Rogers Insurance Canada Ltd.

5 Cyber Safety Tips for Business Travellers

Whenever an employee travels for business, it's likely that cyber security is one of the last things they're thinking about. However, cyber security is not only important in the home and office, but on the road as well. Business travellers are particularly vulnerable, as they often carry multiple devices (e.g., smartphones, laptops and tablets) that all store sensitive data—both personal and company-related.

In order to protect your employees that travel for work, instruct them to do the following:

1. Install antivirus protection on all applicable devices. Keep this software up to date.
2. Lock devices down with a PIN, fingerprint or password. If available, employees should consider using two-factor authentication—a security strategy that is commonly used to add a layer of security to your online accounts by requiring multiple forms of password verification.
3. Be wary of public Wi-Fi, particularly if the network is unencrypted. These networks are highly susceptible to cyber attacks, making it easy for criminals to steal data. If employees must use local Wi-Fi, instruct them to avoid accessing personal accounts or sensitive data while connected.
4. Keep the operating systems on their devices updated. Older versions of operating systems and software often have unpatched security vulnerabilities. Performing a simple update can help keep information safe.
5. Avoid leaving their devices unattended. One of the easiest ways cyber criminals steal data is by having access to the physical devices themselves.

Keeping the above tips in mind can help employees protect their devices and their data whenever they travel.

Why Cyber Incident Response Plans Matter

Simply put, every organization that stores or handles data is at risk of a cyber attack. As technology advances, companies are collecting, storing and transferring more personal information about their customers and employees than ever before. This not only puts a target on an organization's back, but it also means that just one breach can affect thousands or even millions of individuals. And, unfortunately for businesses, cyber incidents cost more than just data:

- **Data breaches are becoming increasingly expensive.** While cyber liability insurance can help offset the costs of a data breach, just one breach can be financially devastating. According to a survey conducted by the Ponemon Institute, the average cost of a data breach was $5.78 million, or $255 per lost or stolen record.
- **Regulatory costs can be significant.** With the advent of Canada's Digital Privacy Act, failing to handle a data breach properly can result in major fines. Companies must comply with mandatory data breach notification and reporting requirements. Failing to do so can result in fines of $100,000 per violation.
- **Cyber incidents can lead to serious reputational damage, significantly impacting directors and officers.** According to Kaspersky Lab, a global cyber security company, a single cyber incident can cause brand damage of $8,000 for small and medium-sized businesses and $200,000 for larger organizations. When wide-scale breaches occur, a company's reputation can be tarnished, sometimes permanently. In addition, the public often holds directors and officers accountable for major losses of personal data.

Acronyms All Businesses Need to Know

In the world of cyber security, it's easy to get overwhelmed with all of the acronyms industry experts throw around in everyday conversation, especially when they relate to unfamiliar concepts. Nonetheless, it's important to become familiar with these terms and understand their general purpose.

Addresses Perimeter and Endpoint Security

IDPS: Intrusion Detection and Prevention System – An IDPS generally involves both an intrusion detection system (IDS) and an intrusion prevention system (IPS). The IDS component contains a database of known attack signatures, which it uses to detect and monitor incoming threats. The IPS component is able to respond to events detected by the IDS.

EDR: Endpoint Detection and Response – An EDR solution is intended to detect and respond to anomalies in any of your endpoints. Endpoints are any devices connected to your network, including servers, workstations and modems.

Addresses Users and Data They Access

UBA/UEBA: User Behaviour Analytics – UBA solutions focus on user behaviour and are an affordable way to detect, report and respond to changes made to your critical data.

DLP: Data Loss Prevention – DLP does the same as UBA in that they both keep track of sensitive data and ensure that it isn't lost or mishandled. Unlike UBA, however, DLP focuses on the data itself—not how users interact with it.

Keeps an Eye on a Broad Range of Sources

SIEM: Security Information and Event Management – SIEM and EDR work together to aggregate data from multiple sources, but unlike EDR—which only monitors endpoint abnormalities—SIEM solutions are able to monitor events from a broad range of sources. Those include your IDPS, firewalls, antivirus software, end-user devices, servers, network traffic and operating system logs.

CCV Insurance & Financial Services Inc
32 Queen Street West
Brampton, ON L6X 1A1
905-459-6066
www.ccvinsurance.com