CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Cybersecurity and Data Protection

TECHNOLOGY SPOTLIGHT

It is 2019. More than 6 million data records are stolen or lost every day.[1] To reduce the damage, $6 trillion will be spent globally by 2021.[2] The latest changes to Canada's privacy law require all companies to invest in data protection.[3] *How will you allocate your security budget?*

Although more than 75% of Canadian companies of all sizes have reported they expect cybersecurity attacks to increase, fewer than half are planning on increasing their security budgets to meet their own data protection and compliance requirements. Few are prepared for the increase in cyberattacks despite the prospect of $100,000 fines for deficiencies associated with data breach notification (PIPEDA[4]), $10 million fines for unsolicited commercial messages containing malware (CASL[5]) and over $60 million in penalties for organizations whose mishandling of the personal information of European residents – regardless of continent – can be a violation of the European Union's General Data Protection Regulation (GDPR).[6] In addition, cyberthreats through the use of malware, phishing, ransomware, and other techniques continue to bring new threats.

1 Since 2013 there have been 6,061,622 records stolen from breaches every day, 252,568 per hour, 4,209 per minute and 70 every second of every day as reported by https://breachlevelindex.com on August 26, 2019.

2 Approximately $6 trillion is expected to be spent globally on cybersecurity by 2021. Organizations need to make a fundamental change in their approach to cybersecurity and reprioritize budgets to align with this newly defined reality of modern society. www.forbes.com/sites/forbestechcouncil/2018/11/09/how-not-to-waste-a-trillion-dollars-on-cybersecurity/

3 www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810.

4 *Personal Information Protection and Electronics Documents Act* (PIPEDA) is a federal privacy law in Canada that sets out how businesses must handle personal information in the course of commercial activity.

5 Canadian Anti-Spam Law (CASL) is a federal law to protect consumers and businesses against spam and electronic threats.

6 General Data Protection Regulation (GDPR) is regulation in European Union law on data protection and privacy that was implemented May 25, 2018.

Across all industry sectors, few managers and directors may be aware that the *Digital Privacy Act* extended PIPEDA's scope to include the requirement to disclose and report data breaches, bringing with it the additional potential for subsequent litigation in addition to the aforementioned fines.

Some Canadian companies are taking full advantage of the opportunity to secure their practices, protect their customers' data and get a leg up on the competition by demonstrating evidence of compliance and adherence to security standards. In addition to requiring organizations to inform an individual when their personal information has been disclosed in a way that could cause significant harm, the *Digital Privacy Act* now requires organizations to keep and maintain a record of all data breaches involving personal information.

But to report breaches, they first have to be detected. Investing in security monitoring capabilities and internal controls is central to a company's accountability for their own data breaches and how they handle them.

Importance

Cyberthreats and data breaches can cause significant monetary and reputational damage. The revised PIPEDA imposes fines up to $100,000 on Canadian companies that fail to properly notify consumers and the Privacy Commissioner of data breaches. As of November 1, 2018, Canadian companies that store, process, control or manage personal information are responsible for notifying the affected individuals.

Companies must act now. According to a recent study,[7] the following statistics show the percentage of companies listing their top reasons for preparedness and security spending:

- 74%: the need to implement or demonstrate best practices
- 69%: compliance mandates
- 36%: responding to a security incident that happened in their own organization
- 33%: mandate from the board of directors
- 29%: responding to a security incident that happened in another organization.

The organizations that are prepared will stand to reap the lion's share of the benefits, including greater competitiveness and increased awareness.

7 2018 IDG Security Priorities Study https://resources.idg.com/download/executive-summary/security-priorities-2018.

Business Considerations

Preparation

A surprising 43% of cyber attacks specifically target businesses and individual accounting professionals. After taking the opportunity for introspection and re-alignment, compliant organizations have an opportunity for contact and dialogue with others in a similar situation. In fact, that opportunity is not limited to business contact; simply contacting the Privacy Commissioner's Office or making an introduction can be a great way to establish an early relationship with authorities, gain access to official resources and get an overall sense that the business is not operating in a vacuum. Each business is responsible for its operations and accountable for its actions, but it already has a key partner in the battle, the Privacy Commissioner, who can offer valuable leadership and resources well before they are needed.

The biggest advantage of preparation lies in the reduction of human error. Ninety-five percent of cybersecurity breaches are due to human error.[8] That high percentage suggests that many cyberattacks are not strictly against the technology; they are against the human factor. In fact, 64% of companies have already experienced web-based attacks; 62% have experienced phishing and social engineering attacks. Therefore, ongoing education and training for employees, such as Cyber Awareness Campaigns and Fraud Prevention Weeks, are very important forms of prevention for a company.

Detection and Monitoring

Canadian companies and sole practitioners now have the opportunity to protect themselves and their customers using proven cybersecurity safeguards; their U.S. counterparts have been familiar with data breach reporting since California's SB1386 law came into effect July 1, 2003. Canadian companies, however, are only now discovering the legal requirement to detect breaches in order to report them to the Privacy Commissioner and notify victims. The current challenge for Canadian companies is to bridge a 16-year gap in risk maturity to catch up to their U.S. counterparts.

With the total cost for cybercrime committed globally calculated to be over $1 trillion dollars in 2018,[9] the detection rate for data breaches has been very low. In fact, the average time to detection is 191 days. This is an unacceptably long time for victims to wait before being able to react to protect themselves in the future. Canadian companies now must adopt measures to monitor and detect security incidents as quickly as possible so they can react to them and correct the situation. Such detective measures include but are not limited to:

8 95% of cybersecurity breaches are due to human error. Cyber-criminals and hackers will infiltrate your company through your weakest link, which is almost never in the IT department. www.cybintsolutions.com/cyber-security-facts-stats.

9 www.cybintsolutions.com/cyber-security-facts-stats.

1. **Managed Security Service Providers (MSSP)**
   Most IT support companies now offer the ability to professionally monitor network equipment, devices and applications to ensure they remain secure. Small and large MSSPs can supplement or even replace existing IT departments. This frees up internal resources to focus on running the day-to-day business by outsourcing technical activities to professionals.

2. **Intelligent firewalls**
   These devices are often built into network routers and other equipment, enabling small enterprises to be notified of breaches as they happen or to review access logs after the fact. With the ability to recognize intrusions and not just block network traffic from undesirable sources, these firewalls are smart enough to record and pinpoint attempts to breach security with far greater precision than before. The caveat is that they themselves must be updated, configured and monitored properly in order to be trusted to protect company assets. For added security, small and medium-size enterprises (SMEs) should select firewalls with intrusion detection *and* intrusion prevention capabilities built in.

3. **Memory resident antivirus**
   All current anti-malware technologies now continuously scan the computer's memory for gremlins and automatically disinfect it. Established antivirus software from brands like Norton, McAfee, and F-Secure can provide centralized control and visibility across the company's entire network. So even small enterprises have the added option to manage security centrally. Market-leading tools also include anti-ransomware, anti-keylogging and rootkit protection to prevent and detect some of the most damaging infections threatening modern enterprises. With an estimated 10 million new strains of malware introduced into the Internet ecosystem each month,[10] businesses need all the help they can get.

According to 56% of IT decision makers, targeted phishing attacks are their top security threat, even as 92% of malware is delivered by email.[11] This places a focus on email security, spam filtering and anti-malware scanning of all messaging, including chats and other forms of digital communication.

Notification and Reporting

While detection is the biggest technical challenge for Canadian companies, the decision to notify based on the test for "real risk of significant harm" is management's primary hurdle. It places the responsibility on management to understand the impact of the breach and take appropriate action to notify potential victims, report the event to the Privacy Commissioner of Canada, or simply secure their systems if they determine the risk of significant harm from the breach is minimal.

10 AV-Test.com Malware Statistics June 2019: www.av-test.org/en/statistics/malware.

11 Top cybersecurity facts, figures and statistics for 2018 www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html.

Risks and Associated Countermeasures

Risks (what could go wrong)	Countermeasures (mitigation and remediation strategies)
INTERNAL AND WORKPLACE RISKS	
Teleworkers are more susceptible to hacks because they connect in diverse environments. **Employees with portable devices may introduce malware into the business environment.** **Loss of mobile devices can create a serious data breach that must be reported and may result in public embarrassment.** **Personally-owned devices do not meet the organization's standards.**	• Provide secure access to the enterprise's systems and data such as through VPN, encrypted channels and virtualization environments such as those available from VMware and Citrix. • Ensure only approved devices connect to the corporate network and that they are automatically scanned when they connect. • Implement procedures to disable use and delete data from lost or stolen mobile devices. • Set policies to define expected behaviour as well as the consequences of not following the policy. • Corporate applications should be encapsulated or compartmentalized separately from user applications and data.
MALWARE AND ACCOUNT TAKEOVER	
Employees accidentally download and install malicious software. **Employee provides personal credentials in response to an email hoax.** **Employee follows a hyperlink on a web page or in an email message that leads to a page that attempts to use browser's vulnerabilities to install malware.**	• Ensure all downloads and web browsing activities are filtered for security. • Block Internet access to known phishing or attack sites and use pattern-based filtering to identify unknown sites or unusual activity by installed applications. • Restrict users' ability to download and install software or software updates.
NETWORK SECURITY & ACCESS CONTROL	
Remote access activity is unexplained. **Network activity and high traffic use are unusual.** **Web communications, DNS resolution and user agent strings are unusual.**	• Test and deploy network security updates from all vendors. • Carry out periodic penetration tests. • Hosts attempting to establish a communication channel using DNS requests to unknown DNS servers, trying to connect directly rather than using an enterprise web proxy, or using non-standard user agent strings such as one that includes the internal host name, may be signs of advanced persistent threat activity and should be investigated.

Conclusion

Cybersecurity and data protection are important not only to large corporations but also to small and medium enterprises (SMEs). Cyberattacks can result in significant financial penalties and reputational risk. Businesses need to provide standardized employee security-awareness training programs. It will help employees detect and prevent security breaches in all aspects of their roles. This will help with cybersecurity countermeasures and mitigate risk in all aspects of corporate operations.

The above table is a handy reference to the top cybersecurity risks and strategies relevant to small businesses and accounting practitioners. To go beyond these recommendations, we recommend the resources of CPA Canada and the AICPA including the SOC Guide for Cybersecurity. Additionally, industry best practices have been standardized in such guidance resources as the CIS Critical Security Controls, the NIST Cybersecurity Framework, ITIL security management practices aligned with ISO 27001 and the control objectives of the COBIT (Control Objectives for Information and Related Technologies) framework, from ISACA.

This publication is part of the **Technology Spotlight series**.

The entire series covers technology trends that impact CPAs and are available on our website.