3 WAYS TO MAKE STRATEGIC INVESTMENTS IN CYBERSECURITY

The importance of managing cyber risk is well-known, and Canadian organizations already demonstrate a willingness to invest in it. But putting resources into security isn't enough. Companies must ensure their investments are strategic and meaningfully improve their security profile.

First, it's critical to understand your organization's obligations to keep customer information secure and private. This will help shape your policies and practices. Second, recognize that your employees are both your greatest security vulnerability and, with the right approach, your greatest security defence. Finally, consider engaging a partner with expertise in security management that can help you design a thoughtful, effective security program that makes sense for your organization.

1. KNOW YOUR OBLIGATIONS TO PROTECT CUSTOMER PRIVACY.

The European Union's establishment of the General Data Protection Regulation (GDPR) in 2016 impacted many Canadian companies that do business internationally. In Canada, privacy regulations are less strict by comparison. They're also inconsistent, with requirements varying by province.

This variability exists despite the Personal Information Protection Electronics Act (PIPEDA), which regulates how Canadian companies collect, use and disclose personal information. Unlike regulations in other jurisdictions, PIPEDA does not have a mechanism for imposing fines directly. Instead, it uses an ombudsman model. Complaints be can be taken to the Office of the Privacy Commissioner of Canada, who then investigates, produces a report and makes a recommendation about whether there should be a penalty and what form it should take. But this recommendation is not binding. The complainant can bring the report to the federal government and request a hearing, a process that can result in penalties.

Complicating Canada's regulatory landscape is the existence of provincial laws that are, in some cases, more stringent than the federal PIPEDA. In Alberta, the privacy watchdog has been able to issue fines and order corrective actions since 2014.

But PIPEDA can't and shouldn't be ignored. In 2018, it was updated with stricter requirements for businesses. Worryingly, a report from the Canadian Internet Registration Authority (CIRA) found that while 59 percent of respondents store personal information, just 38 percent were familiar with PIPEDA's pre-2018 requirements, and 42 percent were aware that the requirements were changing.

Canadian organizations must report breaches of personal information to the Privacy Commissioner of Canada, keep records of the breaches and notify individuals affected. Putting aside the confirmation of possible fines and penalties, these requirements should inform your security practices. You must ensure you have a process in place for recording breaches and reporting them to the commissioner. Meeting your obligations at the outset will put you in the best possible position, whatever might occur.

It's an offence to knowingly fail to meet PIPEDA's record-keeping and reporting requirements. If the Attorney General of Canada chooses to prosecute a case, possible fines range up to CAD$100,000.

That figure is insignificant when compared to penalties imposed elsewhere. For example, the 2017 Equifax breach prompted US$700 million in penalties in the U.S. In Canada, only the Ontario Privacy Commissioner made recommendations. Most of these were accepted by Equifax, but the company refused to offer a credit freeze product that would help prevent fraudulent inquiries into personal credit scores. Equifax did agree to provide four years of free credit monitoring to Canadians impacted by the breach — but was not required to pay a fine.

While the financial penalties in Canada might seem inconsequential, there are other reasons to comply with PIPEDA. After all, bad press, losing the trust of customers and partners carry their own costs.

2. INVEST IN EMPLOYEE TRAINING TO PREVENT BREACHES.

Companies can be so focused on other aspects of securing their businesses that they overlook training their own staff in cybersecurity best practices. According to Statistics Canada data collected in 2017, 51 percent of Canadian businesses share general cybersecurity practices through email, bulletin boards or employee information sessions. Only one percent provide formal training to develop or upgrade security skills. The study also underlined the challenges faced by small businesses: large businesses were more likely to train their staff (59 percent), while just 32 percent of medium-sized and 16 percent of small businesses provided training.

Why does this matter? Employees have access to your business's systems — and that makes them targets of choice for hackers. In fact, phishing is the most common kind of cyberattack. If an employee takes the bait in a phishing attack, by clicking a malicious link in an email, it can infect your systems with ransomware, or lead to the theft of personal and proprietary information.

The good news is that these attacks can be prevented by fostering safe online behaviour through training.

An Accenture survey found that 19 percent of respondents weren't sure how to identify a phishing email. But 70 percent of people who received cybersecurity training said that it improved their ability to recognize threats and react to them.

When training employees, it can help to frame the process as part of strengthening the company's overall security posture. Make the connection between security training and the company's ability to carry out its business without interruptions, losses or loss of customer and public trust.

Don't just share this message and training with lower-level staff. Just as companies can overlook the importance of engaging employees, they can also be too narrow in their scope of who requires education.

Leaders in a company are just as vulnerable to cyberattacks as their teams – perhaps even more so. Also look beyond your internal staff to everyone that engages with your IT, including contractors and service providers. Breaches that impact them can in turn impact you.

Consider offering or even requiring that they participate in security training, for everyone's benefit. The Canadian Securities Administrators (CSA) found in a 2016 study that 90 percent of firms use services provided by third-party vendors, but only 57 percent explicitly address cybersecurity with those vendors in written agreements.

These efforts to improve your security posture – thoughtful, preventative and inclusive of all staff and partners – are the kind of strategic, smart investments that will enable you to reach your business goals.

3. ENGAGE A PARTNER WITH SECURITY EXPERTISE.

Expanding and improving your security capability can be done in several ways. Adding staff is one: 28 percent of Canadian businesses plan to add cybersecurity staff in the next year, according to the CIRA report.

Another approach to consider is working with a partner such as CDW Canada that can provide services and advice that are flexible and scalable to your changing needs. These approaches aren't mutually exclusive. A combination of new staff and assistance from a committed partner might be what's right for you.

No matter your industry, CDW's security experts can assist you at every step of your security journey. They can help you navigate your compliance requirements to truly secure the information your company stores. They can also work with you to design a security program that addresses the gaps in your security posture.

Filling those gaps might involve ensuring your data is securely stored off-premises, that your cybersecurity software and services are working together to detect, identify and stop threats, and that the hardware your employees carry is properly encrypted in case of loss or theft. Of course, our experts can also help you educate your staff about cybersecurity and what they can do day-to-day to protect your business.

Your risk profile can and will change over time. As your partner, CDW Canada will make sure your IT solutions meet your needs as you grow and the threat landscape evolves.

OUR PARTNERS

To learn more about how CDW can help you achieve your IT security objectives, contact your CDW account manager at 800.972.3922 or visit CDW.ca/security