Rogers Communications and IDC Present

The Cybersecurity Guide for Canadian Businesses

An IDC White Paper
Sponsored by Rogers Communications

David Senf, July, 2017

IDC
Analyze the Future

Executive Summary

Everyone in your organization needs to be thinking "security."

Cybersecurity is consistently ranked as a top-of-mind concern for Canadian organizations. Yet many are daunted by the complexity of it, and often unaware of the best practices that can reduce risk, if not fully block attackers from accessing sensitive data or otherwise disrupting their organization.

This guide is here to help. It's designed to teach Canadian small and midsize organizations where to begin and how to create a successful plan to combat continuous cyberattacks aimed at employees, smartphones, PCs, back-end servers, and all other devices and systems, including social networks and IoT sensors. It also offers information about how and where to apply security tools and techniques. Everything is explained in straightforward language for business professionals and non-security experts.

The guidance provided in this handbook is based on IDC's extensive Canadian security research that spans decades. The ultimate goal for your organization should be to develop security best practices within your culture and encourage behaviours that become routine, like good "**habits**."

Because too many organizations aren't doing enough to protect private information, Canadian **privacy** laws are becoming even more strict in 2017. Additional fines are being imposed this year to encourage organizations to do more to safeguard personally identifiable information (PII) of employees and customers. Chapter 4 of this guide contains details about privacy plus other legislation and regulations of which you need to be aware.

Canadian organizations struggle to find, recruit and retain **security talent** because of an extremely limited labour supply and the large demand for security professionals. Small and medium-sized organizations often don't have the budget for in-house security experts, so outside providers and security communities offer capable alternatives. Chapter 5 includes a summary of resources where you can find security talent, local and online security communities and learning opportunities.

To safeguard your company data and keep business operating as usual, you should make and follow a **security risk plan**. It will help you determine how to allocate your security budget effectively. Setting up a basic risk plan is explored in Chapter 6.

IDC research shows Canadian small and medium-sized businesses generally underinvest in IT security. A **security budget** should represent approximately 10% of your total IT spend. Our research also finds that merely buying more security technology often doesn't markedly improve security. Your budget also needs to include spending on activities such as employee training and device monitoring. See Chapter 7 for more details on security budgeting.

Unfortunately, there is no one **security technology** or solution that can completely eliminate the many different kinds of attacks your organization faces. You'll find a detailed list of 10 critical areas that attackers typically target and some suggested security technologies that should be a part of your defence in Chapter 8. However, employee training should be your first line of defence against cyberattacks.

Training employees on security best practices is among the simplest and most cost-effective ways to reduce the likelihood and impact of a security incident. You need to educate employees about how to keep sensitive data secure and how they should use that data – safely – in their day-to-day work. Employees not trained in security best practices is a top weakness for most Canadian organizations, according to IDC research. Employee training is detailed in Chapter 10.

IDC research shows four out of five Canadian organizations are likely to experience some sort of security breach this year. Nearly half will experience a major incident resulting in part from their business being taken offline and/or sensitive data being accessed by attackers. You need an **incident response plan** to react quickly and minimize the impact when this happens. Like your security risk plan, an incident response plan must be a critical part of your security strategy. Once detected, an incident needs to be contained and eradicated from your systems and devices. Chapter 12 provides the basics of security incident planning and response.

61% of Canadian organizations will take months if not years to even know they have been breached

Creating a more secure organization takes time, effort and dedication. This guide will help you assess the effectiveness of your risk planning, technology, training, monitoring and response plan. IDC suggests reviewing the material in this guide on an annual basis at least. Establish a timeline for implementing security improvements in the manner outlined in Chapter 13. Also in that same chapter, discover your organization's **security maturity** to understand the current state of it and to have a baseline to measure your progress and success.

Finally, make security a priority by putting someone in charge. **Leadership** is key to making headway on reducing security risks. You can't afford to slip backwards. You need an "owner" for your organization's security – a strong leader able to turn cybersecurity knowledge into best practices and habits.

Chapter 1

Introduction

Cybersecurity should never be taken for granted – and the Canadian government has put stricter rules and fines in place to ensure it is taken more seriously. Attackers are "casing your business," surveilling it, looking to discover potential entry points and weaknesses. Too many Canadian organizations are allowing attackers to sift through their private data on their website, smartphones, laptops and network because they haven't put the right security defences in place. You need to make a plan, deploy the right solutions, monitor for attacks and train employees to be vigilant.

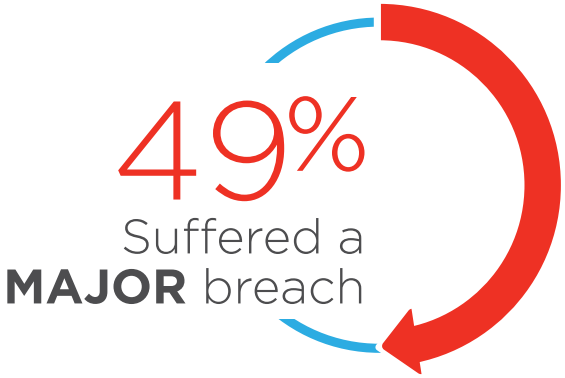
Cybersecurity evokes the picture of a dark and shadowy world full of intrigue, mystery and detective work needed to track down villains. But it's easier than you might think to establish the fundamentals of sound security practices to steer your organization in the right direction. It's a matter of finding the most cost-effective ways to deter attackers.

Attacks against your organization will come in a number of forms:

- It can be as obvious as a glaring ransom notice on an employee's screen demanding money in exchange for the keys to unlock their data.
- An attacker may disrupt your business by denying customers or employees the ability to access websites or other applications.
- They may want to steal processing power by tapping into your smartphones, PCs or servers to launch attacks against other organizations.
- Other attackers may be motivated to deface your brand or slow your business down.
- Usually an attacker is looking to profit from acquiring valuable information – such as social insurance numbers, health information, credit card numbers, financial data and other company secrets.

Whatever form an attack takes, the end result is about the same – you've lost money from the bottom line or have had services disrupted.

Security professionals admit



Security breaches – meaning an attacker has found a way into a smartphone, PC, server or cloud service you use – are quite common. IDC finds that many security attacks go completely undetected by organizations while an attacker has free rein to move through a business's data. IDC research finds that 61% of Canadian organizations will take months if not years to even know they have been breached, let alone fixing the problem. This is the reason that millions of records of private and personal data will be exposed in Canada this year.

No Canadian organization is fully prepared to stop a security breach. In a recent survey of security professionals IDC found that 83% reported a minor breach at their organization resulting in at least one employee being disrupted from working. The survey also showed that 49% reported a major breach where funds were stolen, private data exposed or any number of other losses were incurred.

Although learning the basics of cybersecurity is not complicated, it is not as simple as loading some antivirus software on a PC and installing a firewall on the network. Nor can you merely "set it and forget it." Devices and systems need to be continually monitored for new threats.

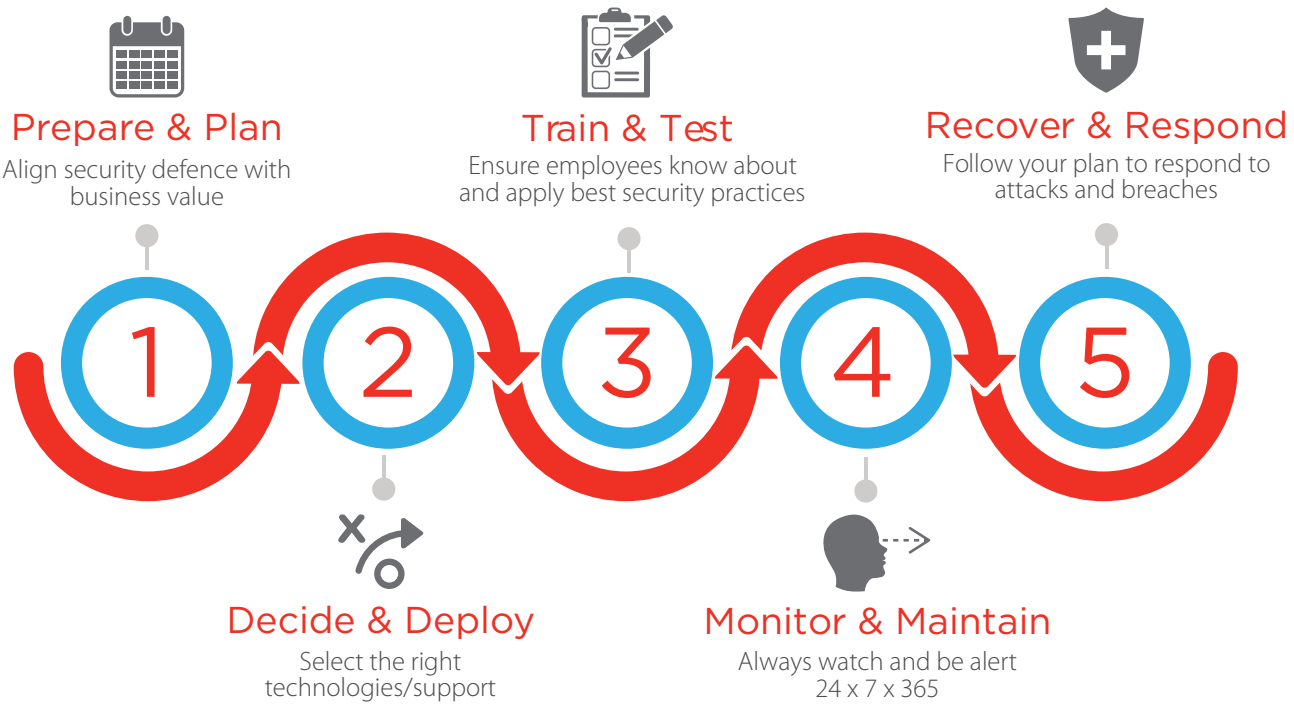
In This Guide

Very few easy-to-follow guides exist that are dedicated to helping businesses understand what needs to be done to avoid becoming a victim. We're here to remedy that. This handbook highlights the cybersecurity threats that businesses face today and provides the key ingredients to serve as a recipe for how to keep your business safer. We're writing this for the small to midsize firms that represent the vast majority of businesses in Canada – the foundation of our country's economy.

There's no need to burn the midnight oil reading this guide cover to cover. We've assembled it into digestible morsels that can be consumed conveniently and quickly. If you're not a hardened security veteran, not to worry – we've written this content to make otherwise complex concepts and strategies straightforward for business professionals with any number of diverse skillsets.

IDC has for decades assessed and studied the IT and cybersecurity threats faced by organizations across Canada and around the globe. Throughout this guide, we'll draw on that research to help you understand the major risks and vulnerabilities, and how to implement the IT and cybersecurity framework that has been developed by IDC Canada – the "**5 Habits of Highly Secure Organizations**." Warding off attacks, mitigating risk and minimizing the impact of IT and cybersecurity breaches for your business is akin to doing the necessary things to maintain good health – it is all about adopting a set of good habits and practices.

Highly secure businesses follow these **five habits**:



Fivehabit summary

Habit	Action	Result
1 Prepare & Plan	Consider what is most important to protect in your business. Make a plan to prioritize what needs to get the most attention, to what degree these assets should be protected, and how much is appropriate and reasonable to spend.	**Spend the right amount in the right places**
2 Decide & Deploy	Select the most effective tools and solutions to protect the most important parts of your business. Then figure out the best ways to put these technology and managed services in place.	**Buy only the most appropriate solutions and services**
3 Train & Test	Share the details of your plan your employees must know and follow, and instruct them on what they need to do. Train your staff.	**Reduce the likelihood of staff becoming the greatest security risk**
4 Monitor & Maintain	Keep a constant eye on the protection tools and practices put in place and ensure they continue to be effective and meet your business needs. All software should continually be updated with the most current versions available. Likewise update operating systems on smartphones, PCs, and connected devices throughout your business.	**Adapt to changing threats and monitor risks to make changes when needed**
5 Recover & Respond	Know how to minimize the impact of a breach and quickly get back to business as usual. You need an incident response plan in order to guide you.	**React quickly and effectively to minimize the impact**

This guide can be used to create a security roadmap and offers basic benchmarks to help ensure you remain on track. Effective security is about being proactive and action-oriented toward potential threats against your organization.

Chapter 2

What does it mean to be secure?

More than 5.1 million personal and private data records of Canadians will be exposed by an attacker this year. IDC research also reveals that small and medium businesses often believe they are not a target for cybersecurity attacks and won't themselves be victims of data being compromised. The truth is every business is a target and IDC research shows small and midsize businesses are exposing more sensitive data than larger firms. Medium-sized businesses, for example, employ 23% of Canadians, but are responsible for 42% of personal private data being compromised.

Big businesses are more likely to follow best security practices as well as the many habits explored in this guide. The most secure Canadian organizations invest in a range of solutions to defend themselves. One key difference separating the most security-conscious from others is the effort and investment made in training staff in the appropriate security practices. IDC research in Canada shows that the greatest cause of data theft is a result of employees being tricked, phished or otherwise coerced into revealing login information or sensitive data itself. Training is key to improving employee knowledge and behaviour. Please see Chapter 10: "What Should an Employee Training Program Include?" for more detail on employee security training.

Nothing is ever 100% secure. But by following good security practices and habits (e.g., security planning, using the right technologies, training staff and continuous monitoring) businesses are able to slow down an attacker – and that may be enough to prevent a breach. Attackers work to find any weakness in order to gain entry into your PCs, smartphones, servers, cloud deployments and any connected device to access the information they want. Your goal should be to make it as difficult as possible for attackers to find an entry point into your customer, financial, employee and other data. Even connected HVAC systems, printers or networked sensors can be used by an attacker.

TOP 10
Security Holes in Canada

According to Canadian organizations most likely cause of exposed data

1. **Employee error / attacker tricks**
2. **Email**
3. **Removable media** e.g. USB Key
4. **Laptop**
5. **Smartphone**
6. **WiFi**
7. **Web application**
8. **Tablet**
9. **Desktop**
10. **Public cloud**

Think like an attacker

It is helpful to understand how attackers think. Like many business people, they look to drive the most revenue at the lowest cost and effort. So, the more difficult it is for an attacker to access your valuable information, the better your chances of discouraging them and reducing the risk of their success.

Some attackers scour the internet, casting nets as wide as possible to retrieve any information of value. They employ readily available tools to find weakness in your defences with very little effort. The scouring process

is often automated and similar to randomly dialing phone numbers until someone answers. Attackers use tools that "call" internet addresses to find any connected PC, smartphone, web server, sensor or any other device. They then deploy malware (meaning any software that causes harm) or other attack method to record your keystrokes, locate data or learn what services you use (e.g., which suppliers your business contacts so they can mimic them and ask for bill payment). Like any mature online business model, the tools of the cyberattack trade are readily available even to novices.

Attackers assemble large volumes of stolen data into bundles that are sold for just a few dollars on the black market to criminal organizations. It has become a high-volume/low-margin business as more small-time crooks and large criminal organizations are getting in on the action. This has the effect of driving down prices for stolen information and data. For instance, a person might purchase bundles of 1,000 hacked email accounts for less than a dollar. Similarly, valid credit card numbers can be purchased for as little as $0.50 per card (prices fluctuate depending on credit limit and other factors). Bottom line: Cybercrooks require more data to keep their nefarious industry in business as the price of stolen data continues to drop. In retail, some cybercriminals are using malware right at the point of sale, while others try to gain access to internal IT systems through employee error, carelessness or, sometimes, malicious intent.

Modern day attackers use a somewhat standardized approach:

- An attacker sizes things up, using publicly available information to learn about a target. The attacker considers – is there anything of value here? Are there easy ways to gain access to it?
- An attacker finds a target and identifies weaknesses and easy entry points.
- The attacker chooses a point of attack and goes for the breach. A best shot will be taken at accessing protected information or getting a foothold behind your defences.
- Once a successful penetration behind a target's defences has been established, the attacker will dig deeper seeking to take gain control of systems.
- After grabbing everything of value and deciding there's nothing left to be reaped, the attacker withdraws, covering any footsteps or evidence of their presence.

Once inside your systems, attackers are in a position to deliver the payload – typically malware in the form of an infected file or a piece of software that allows an attacker to gain remote control of your devices and/or applications without your knowledge.

Three common types of malware are:

Ransomware
An increasingly common variety of malware, ransomware works by using encryption against you, to deny you access to your own data and information. The attacker locks up your important files and asks for a ransom to be paid in order to restore access. Often, they demand to be paid electronically in Bitcoin so the transaction can't be easily traced.

Keyloggers
This type of malware is so simple it's almost elegant. Keyloggers capture everything typed on a keyboard, including usernames and passwords. For an attacker, it's simply a matter of sitting back and waiting until crucial information about your business has been keyed in.

Trojans
Like the infamous Trojan Horse, the payload of this attack is disguised as something trusted that you'd be apt to open as a file or run as an application. But in doing so, a hidden file or application is released on your computer and becomes the open gate for all sorts of invaders to come flooding in and wreak damage by compromising or stealing your data.

A wider variety of threats and how to defend your organization against these can be found in the section entitled "Where to Start?"

Attackers Open 24 x 7 x 365

Your organization needs to defend itself with a 24 x 7 vigilant mindset to counter attacks.

Attacker approach	Your action
Up and running 24 hours a day, 7 days a week	Be on guard all the time, 24/7. Have defenses in place that are always on. Stop a breach before it happens. Know how to recover quickly if it does.
High volume of attacks, low margin business	Protect high-value company, employee and customer data. Being a smaller business does not mean you won't be a target.
Use common and inexpensive platforms and tools to carry out their attacks	Remain up-to-date and vigilant with your ongoing defenses and training.
Work through worldwide teams that specialize across different tasks	Consider all the ways in which they can gain access to your most important data.
Quickly scale up and shut down	There is little to no ability and recourse for you to recover stolen data. Expand security protection as your business grows.
They are global	You likely won't be able to prosecute them. Continuously secure and guard all entry points.

Chapter 3

What Is Cybersecurity?

Cybersecurity is a set of guidelines, practices and tools for the protection of your electronic data and should be a part of your overall security strategy. Attackers from around the globe use the open networks we all rely on to expose and corrupt data, interrupt business and deface brands. Cybersecurity is among the top concerns for executives and business owners in Canada.The rise of cloud computing, mobile smartphones and all kinds of networked sensors embedded in a wide range of things has resulted in an explosion of data traveling across networks – and potential targets for attackers.

IDC asked organizations across the country which factors will contribute most to the successful use of cloud, smartphones, IoT and the myriad other new technologies. Security topped the list. In our connected world, cybersecurity can make or break a business.

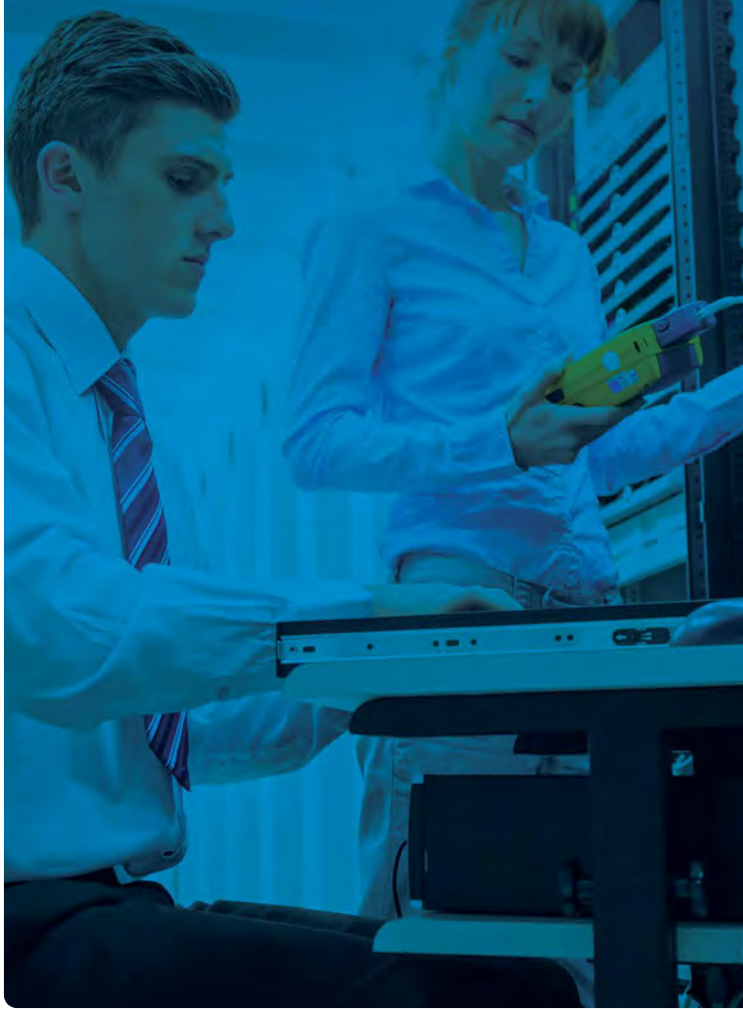
Just like the armoured car that transports money to restock bank machines, you need to develop a plan that delivers tight logistics around how your sensitive data is handled. Consider these cybersecurity basic principles when it comes to handling sensitive data:

- **Data must be secured and monitored wherever it's stored**. Just like the locked-down bank machine under video surveillance, your data should always be stored in an environment that is difficult to breach and encrypted. An alert should be triggered in the event an attack is underway.
- **Data must always be secured while in transit**. That means using technologies like encryption and account verification, often with multiple kinds of authentication, to ensure data in transit from one device to another hasn't been corrupted or won't be stolen.
- **Only data that is needed should be kept and stored**. Bank machines only hold an essential amount of cash based on usage patterns reported. You should only collect and store data that is absolutely needed by your business. Delete data that is not required. Doing so will limit what an attacker might take in the event that a breach occurs. A thief stealing from a bank machine gets only a limited amount of cash.

Follow the data, improve cybersecurity

You need to think like a hacker when trying to protect your valuable data.

Data is like a big bag of cash and you're responsible for its secure handling and delivery. Where might that cash sit for the longest amount of time? When does it have to be moved from one location to another? At what points is its presence most obvious to outside parties? Where might it be most vulnerable to being stolen?



Cybersecurity defences should span the entire range of devices – from PCs, systems, wireless and wired network and anything else connected both inside and outside your organization. The table below shows the top 10 cybersecurity investments made by Canadian organizations based on a recent IDC survey. IDC believes smartphones rank too low on this list and should, in fact, receive much higher investment. Consider how much of your data either resides on smartphones or passes through them via email, a web browser and other applications.

Smartphones are a potential treasure trove of information for would-be attackers and an easy entry point into your network and other devices. IDC believes organizations should spend much more effort securing them. Cloud has gained more attention over the past few years, rising to become the number 2 concern. IDC believes protecting data in the cloud is essential and is a shared responsibility between your organization and the cloud provider. We'll discuss how to protect your information on smartphones, servers, in the cloud and in other places where it may have risk of exposure in the section "Where to Start?"

It's important to look beyond the strict definition of cybersecurity to social engineering, physical and other forms of attacks to reduce your risk of security breaches and ultimately the potential loss of business.

TOP 10
Areas of security investment

1. Server
2. Cloud
3. Wired network
4. Wireless network
5. Web applications
6. Smartphone
7. Email
8. Laptop PC
9. Desktop PC
10. Tablet

Here are a few threats that fall outside of the definition of cybersecurity:

- Theft or loss of a smartphone with valuable information on it
- An employee gets tricked into giving away information over the phone
- A payment card skimmer is installed on a point-of-sale device
- Your business collects inappropriate information from employees

Cybersecurity is the most likely way you're going to be attacked, but these other risks are also important to plan for and consider.

Chapter 4

What Is Privacy and What Are the Legal Implications?

Beginning in 2017, Canadian privacy laws require all organizations to report to the Privacy Commissioner of Canada and customers when a security breach may have exposed personal data. Failure to do so may result in a fine. Even if you don't directly handle customer data, organizations are required under Canadian law to protect employee and other personal private data.

Privacy and security are often spoken about interchangeably, but these are not the same. Privacy is a person's right to control their own personal information. Security is about the technology, training and restrictions that are used to protect that information. Any information that could be used to identify or track a person should always be considered something that needs to be kept safe and secure. The layers of both federal and provincial laws in Canada dictate what kinds of personal data your business may collect, and how it may be used and/or stored. Most countries around the world have similar, if not even stricter, laws.

Here are examples of data and information considered private under Canadian law:

- Age, name, ID numbers, income, ethnic origin or blood type
- Opinions, evaluations, comments, social status or disciplinary actions
- Employee files, financial accounts, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (e.g., to acquire goods or services, or change jobs)

Follow these **10 principles of privacy** as laid out by the Office of the Privacy Commissioner of Canada to demonstrate your organization is working to meet its legal obligations in the event you have a security breach that exposes private information:

1. **Accountability**
   Someone at your organization should be declared as having the responsibility for the protection of customer information, otherwise it is unlikely your legal obligations will be met.

2. **Identifying purposes**
   Ask why the information is being collected in order to avoid gathering unnecessary data. It may limit any potential fines incurred in the case of a breach.

3. **Consent**
   Customers and employees must agree to give you their information.

4. **Limiting collection**
   Don't gather more than you need and avoid expanding legal implications and customer ire if a privacy breach occurs.

5. **Limiting use, disclosure and retention**
   Don't use private data for purposes other than those disclosed to the customer and delete it when you no longer need it.

6. **Accuracy**
   Make sure the information gathered is up to date and complete as customer/employee health, credit and other records change over time.

7. **Safeguards**
   Do what's necessary to protect information by putting the right technologies, monitoring services and training in place.

8. **Openness**
   Share your privacy practices with your customers.

9. **Individual access**
   Always be prepared to respond to your customers when they make requests about the personal information you store on them.

10. **Compliance challenges**
    Be prepared to deal with complaints from customers and the Privacy Commissioner of Canada about your handling of any personal information.

Note that these 10 principles are written with consumer protection in mind, but also apply to employees and any other data you might collect. Any leaked personally identifiable information (PII) could be grounds for fines, a lawsuit or even penalties from regulatory bodies.

The federal privacy legislation and 10 principles are a starting point for improving security and safeguarding privacy. You may also need to adhere to provincial laws and regulatory requirements. Privacy laws in Canada are layered – the bottom foundational layer is for the federal laws that apply across the entire country. The layer above is for provincial legislation, and in certain industries such as retail, healthcare and finance there is yet another layer covering regulations that non-governmental bodies may impose (e.g., the Payment Card Industry standard for cardholder data). Understanding this legislation is a key part of the planning and budgeting (discussed in Chapter 6) process.

Layer 1 – Federal Law

Here are additional details regarding Canadian privacy rules:

PIPEDA and the Digital Privacy Act.
All organizations operating in Canada must comply with the Personal Information Protection and Electronic Documents Act (PIPEDA) and the Digital Privacy Act. Due to the rapid rise of ecommerce, PIPEDA was passed in 2004 to protect consumer privacy and it outlines how businesses need to transfer, store and secure personally identifiable information. The Digital Privacy Act was passed in 2015, and it updated several sections of PIPEDA including new, pending legislation for mandatory breach notification (companies must inform the government when a privacy breach occurs) and establishing penalties for organizations that don't comply. You can expect that the mandatory breach notification and fines will be fully enforced toward the end of 2017. Here are key things you need to know about the new federal law in the event that your business suffers a security breach that could result in data loss:

- **Considering potential harm**.
  Once you determine you've suffered a breach, you are obliged to consider and assess how much risk it poses to the privacy of affected individuals. Factors like the sensitivity of the information and whether it's likely being misused must be weighed here.
- **Reporting to the government.**
  After you've made an assessment and determined there's a risk of harm (a calculation based on the likelihood the attacker can use the information and cause financial, reputation or other loss to an employee or customer), you are obliged to inform the Privacy Commissioner of Canada. As with any government interaction, you'll need to fill out the form the office requires and provide specific information.
- **Reporting to individuals**.
  If the breach does pose a risk of harm, you are required to notify any individuals that have had their information exposed. You'll need to make clear how significant is the risk to that person, and inform them of any steps that should be taken to minimize the risk of negative consequences.
- **Record keeping**.
  Even if you determine there's no risk of harm from the breach, you'll still need to keep a record of it. What's not clear at this point is the sort of detail required in such a record, or how it must be stored and for how long. At a minimum, you'll need to record the date of the incident, the number of affected individuals, specific personal information that was exposed, contact information of administrators of the affected systems and how it was exposed.

For more information on Canada's federal privacy legislation click here https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/guide_org/

Layer 2 – Provincial Law

Here are some provincial laws and guidelines:

- **Provincial law**.
  Alberta, B.C., and Quebec each have provincial legislation to govern privacy that is similar to the federal laws. Businesses in Alberta, for example, are subject to mandatory data breach reporting to the provincial government. Those requirements are contained in the province's Personal Information Protection Act.
- **Health Information Privacy Laws**.
  Ontario's Personal Health Information Protection Act, New Brunswick's Personal Health Information Privacy and Access Act, and Newfoundland's Personal Health Information Act build on PIPEDA for organizations dealing with health information. Other provinces and territories have their own health information registration, but PIPEDA still applies.

Layer 3 – Industry Regulation

Finally, there are industry-specific regulations, including the Payment Card Industry Data Security Standard (referred to commonly as PCI DSS) plus many others directed at accounting, legal, finance and other business segments.

PCI DSS is regularly updated and the most recent 3.2 version was released in the spring of 2016. It has a list of requirements that must be met by any organization that accepts credit cards. The regulation is mainly focused on ensuring credit card data is kept separate from other customer data. Having this separation is intended to reduce potential opportunities for attackers. Failure to accomplish this has led to some of the biggest data and damaging breaches reported in major headlines over the past couple of years. For many small and medium-sized businesses, performing an annual checkup in the form of a self-assessment questionnaire (SAQ) is sufficient to maintain PCI compliance (documents can be found here https://www.pcisecuritystandards.org/document_library?category=saqs#results). Depending on the number of transactions your business processes, it may be necessary to work with a qualified assessor who will create a report. A number of security firms across Canada offer PCI assessment and auditing services, typically alongside other security consulting, managed security services and professional security services.

What if I Operate in the U.S. or Internationally?

Privacy Legislation

When data leaves Canada it becomes subject to the privacy laws of other countries – and ignorance of the law is no excuse. There are compliance obligations governing both the in-country use of private data and the cross-border flow of data from Canada into other nations. Two levels of privacy obligations for digital data exist: 1) domestic obligations for data that is collected and stored within the borders of a single country or region, such as the United States or European Union, and 2) international obligations for data that is collected in one country or region but stored in another, such as data collected in Canada but stored in a datacentre in the United States. The good news is that Canadian federal privacy legislation described earlier is based on a common set of international guidelines, so achieving compliance in Canada means you already have grounding in the basics. The international privacy guidelines are observed by more than 30 countries including the U.S. and European Union members. [http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm].

Similar to PIPEDA, international legislation attempts to limit the collection, use and disclosure of personally identifiable information (please see section 4. for examples of PII). One such shared international guideline is outlined in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and speaks to the need to put security defences in place to protect PII: "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data."

It's important to note that Canada was considered to have weaker privacy legislation than other jurisdictions in the past – this has in part been remedied by the new Digital Privacy Act described in Chapter 4. However, if you do business in the United States, particularly within specific industries, such as health, you may need to increase your security safeguards.

Unfortunately, there is no simple answer to what actions you should take to be compliant with existing legislation. The laws differ by country and don't prescribe which security solutions to purchase or what employee training to conduct. If a breach does occur, or private data was exposed by some other means, you need to have IT security solutions and staff training in place (explained in Chapter 12). It will help to demonstrate you acted to "safeguard" sensitive data. More importantly, in areas of law, seek legal advice from experts to protect your business against non-compliance and avoid penalties of fines and potential criminal charges.

Antispam Legislation

If your organization markets to customers or prospective customers in the U.S., you need to give them the option to opt out of receiving future electronic correspondence from your organization. You can assume that consent is given until an individual clicks the "unsubscribe" link or opts out using another way that you have provided to the recipient. U.S. law is in stark contrast to Canadian law. The Canadian Anti-Spam Legislation (CASL) follows an opt-in approach. This means your organization is required to proactively seek customer or prospect consent in order to send them email, text or other electronic marketing communications. A business can be fined up to $10 million for non-compliance with CASL. The three-year grace period, which began in 2014, expires on July 1, 2017, and all organizations must comply. For a detailed description of and exceptions from the law, please visit http://fightspam.gc.ca /eic/site/030.nsf/eng/00304.html#.

Chapter 5

Where Do I Find Security Talent?

Canadian organizations struggle to find, recruit and retain good security talent because of the extremely limited labour supply of security professionals. IDC Canada research shows nearly six out of ten organizations say they find it difficult or extremely difficult to hire security personnel. Among the options available to acquire talent are to hire, train or outsource.

6 out of 10

organizations say they find it difficult or extremely difficult to hire security personnel.

The following is a list of ways your organization can access security talent:

Hire security staff

- **Post-secondary institutions and trade schools.** Cybersecurity skills are increasing in demand and colleges and universities across Canada are responding to that need by providing a wide range of diploma programs and training courses. If you're interested in hiring an intern or onboarding a new graduate, consider getting in touch with local colleges and universities to find specialists who are enrolled in relevant security programs. For internships, coordinate with the faculty department or cooperative education office. To hire a new graduate, get in touch with the school's event department to learn about participating in a job fair, or posting your opportunities for work to school job boards or advertising through email list.

- **IT security communities.** Several specialized groups are located across Canada, though typically concentrated within larger urban centres. These communities provide good opportunities to meet IT security professionals. A list of some of the groups is provided, below.

- **Online and traditional talent and job board services.** A range of recruitment options exist to fill open IT security positions at your organization. Traditional recruiters are one option as are a growing list of online services such as LinkedIn and ZipRecruiter. One of the most expedient ways to determine whether a candidate has a well-rounded knowledge of IT security is to check for the CISSP certification (described below). The downside is that these professionals typically command a higher salary.

- **Staff augmentation and CISO for hire.** Many IT security services organizations offer professionals who can be commissioned for work, based on hours, days or months at a time, depending on your requirements. Specialists in these organizations typically offer skills ranging from general level security knowledge to specific expertise in security processes and practices (e.g., incident investigation, vulnerability detection, identity management and compliance).

Train your IT/security staff

- **Continuing education programs**. Universities and colleges are supporting the growing interest of working professionals in these programs, so they've designed these with flexibility in mind. Evening and weekend classes or study-on-demand online courses are becoming the norm, and programs are often divided up into small segments, sometimes allowing individuals to earn certificates of achievement after only a few months of study.

Train your IT/security staff -continued

- **CISSP and other security certifications**. The most common certification in security today is the certified information systems security professional (CISSP) designation. The 10 areas of focus covered in the CISSP program provide a comprehensive foundation for learning how to protect information assets. Online and other training options, examinations and annual requirements are available to maintain professional status as a qualified CISSP. IT security is part of other frameworks and certifications as well, including ITIL, ISO 27002 and COBIT.

- **Online training and "how to" videos**. "Do-it-yourself" training exists for those with a strong background in IT security acquired from formal training in the past. Programs and podcasts such as This Week in Security are extremely valuable as a means for keeping up to date on latest threats to watch out for, but understanding these often requires a strong foundation in IT security from formal schooling.

Outsource to a security provider

- **Managed security services**. A managed security service provider has the security operations centre and staff to become your outsourced security team. These external service providers gather capabilities from their experience with many clients and threat sources, using that technology knowledge and intelligence about ongoing attacks to continually improve their services and offerings. External service providers have the tools, always-on monitoring and skilled security staff to manage the IT security of organizations – around the clock, every day of the year. A recent IDC Canada survey found that customers say the top reason for selecting a managed security service provider (MSSP) is the 24 x 7 x 365 coverage offered – a particularly important consideration for small and medium-sized organizations that may have limited or no security staff. The average Canadian small business has only a part-time security headcount on staff (e.g., 0.5 of a full-time IT headcount). Typically, this is a person who directs most of his or her time at tasks not related to security – stepping into the role as best they can when needed.

- **Hosting**. These service providers offer secure off-premise datacentre and network facilities and managed connectivity for your servers and applications. Instead of your organization housing hardware and applications on your premises, the external provider is contracted to house and potentially manage IT for you. In a basic arrangement, they'll provide physical security so servers are protected from unauthorized handling or theft. Or a hosting service company can take on nearly all security responsibilities, including the network, server and applications, depending on how much IT control your organization wants to outsource.

- **Cloud**. Similar to the value proposition of hosting, security is a standard feature or element of many cloud offerings. However, your organization must retain responsibility for some IT security elements. Cloud services for applications such as email, sales management and accounting offer most security included within the service. But be mindful that a cloud service may not provide all the security you need. For example, providers don't offer complete user account management (e.g., when an employee leaves your company, you, rather than the provider must recognize this change and switch off the employee account) or data loss prevention (e.g., preventing sensitive data from being leaked by employees). Also note that infrastructure and platform cloud services require you to manage even more aspects of IT security (it provides more flexibility, but in return there need to be more safeguards such as firewall, intrusion detection and log management).

Hire and Learn From Peers in Security Communities

Here's a great idea – meet and get involved with local security groups and associations. These organizations offer knowledge sharing and ideas with peers that keeps security skills sharp. It's also a safe environment to share best practices with other businesses, and even maintain formal certification for your security staff.

Notable groups across Canada:

Toronto Area Security Klatch
A free group that meets on the last Wednesday of each month.

Meetup.com
Groups and events – a quick search for IT security events in your local area can turn up new opportunities to learn.

Canadian Centre for Cyber Risk Management
Based in Waterloo, Ont., is an association with membership that includes businesses, colleges and universities, and industry associations.

Gaming Security Professionals of Canada
A not-for-profit organization that represents major gaming organizations from British Columbia to Nova Scotia. It has educational resources available for casinos and sports betting companies.

Canada's Association of Information Technology Professionals
Based in Mississauga, Ont., also has organized activities for memberships in every province as well as local chapters in many cities across Canada. While not limited to IT security, the group organizes educational sessions, seminars and conferences, plus more informal get-togethers. IT security professionals can also pursue certification through this organization.

National Cyber-Forensics and Training Alliance
Based in Montreal, has labs and training centres located at Concordia University. Dedicated to investigating cybercrime, the organization also offers online resources for learning more about cyberthreats.

The Canadian Cyber Threat Exchange
A not-for-profit organization that helps businesses detect and defend against cyberattacks by sharing information among members. The Exchange also interfaces with other global threat sharing centres.

Online security discussion groups.
Through LinkedIn and other business and community sites there exist local and international discussion forums where participants may post and respond to security-related questions. A search in LinkedIn for "security groups" reveals a number of general and specialized groups tailored for more and less technical, executive, and admin level members.

The good news is that in the high-demand, low-supply labour market for security talent, other options exist. Smaller organizations may not have the budget for in-house security staff, and might instead consider a managed services and cloud-based services option to shore up defences. The security capabilities of midmarket organizations in Canada are typically understaffed as well. IDC research shows strong uptake by midsize Canadian businesses of managed security service to fill security gaps. Ideally, an organization has a trusted security advisor either on staff or brought in as required. Remember, security is everyone's job and the right talent is only one piece of the puzzle. All staff require IT security training.

Chapter 6

What Parts of My Business Are Most at Risk?

Knowing where to invest your security dollars and where to focus your effort is the first place to start. Every device on the network and throughout your organization should be protected to some degree. But some parts of your business may require additional layers of security. There is nothing more important in security than a basic understanding of risk because you won't otherwise know where to put your security defences. The basics can be learned quickly and easily, and applying them within your organization can be simple.

Some data has greater value and needs to be kept confidential – such as company intellectual property, customer credit card information or employee records. Other data, such as marketing material, user manuals or instructional or sales information that your business has created, may be designed to be shared with as many people as possible. Don't spend a disproportionate amount of limited budget defending less sensitive data. Better instead to focus on using the bulk of security funds on protecting the sensitive data.

A security budget should amount to approximately 10% of your total IT spend (the Canadian average budget allocated to security is 9.8%). Risk planning allows you to determine how best to then divide the available security dollars for optimal protection. The largest share of the budget should be directed at the higher-value data assets while a smaller portion might be dedicated to protect lower-value data. Next, identify which data requires what degree of protection, where that data resides and how vulnerable it is to attackers. Each security technology and monitoring service purchased or any staff training conducted reduces the likelihood of an attacker getting at valuable data.

Fewer than one in three Canadian organizations makes and follows a security risk plan

Those that don't typically suffer far more breaches, according to IDC research. More than half of Canadian small businesses say they would grade themselves a B-minus or lower on their security planning efforts, while many give themselves a failing grade.

Fewer than one in five small businesses and fewer than one in 10 medium-sized organizations give themselves an A.

IDC research concludes far too many organization take a "good enough" approach to security as highlighted by these low marks. Even to meet compliance requirements such as PCI (e.g., for securing credit cards), some organizations will deploy the bare minimum of protection. However, IDC research further shows organizations that take the time to plan their security investments carefully, and allocate the appropriate budget to the right defences, suffer fewer breaches than their peers.

IDC finds that medium businesses struggle more than smaller counterparts with security planning because of the greater scope and complexities of their security challenges. Furthermore, they suffer the same financial resource constraints of smaller organizations.

Evaluate your organization's risk

The simple process described below can help your organization evaluate which business functions and sources of information are the most important and where that data resides. Your company can then plan its defences accordingly.

Start by creating a list of the most valuable information your organization keeps. The following are quite common:

- **Financials and accounting information**
- **HR records and employee information**
- **Customer data** (credit cards, addresses, etc.)
- **Company product, process and other secrets**
- **Sales information**
- **Emails**
- **Office productivity documents**

Now make another list of all the places where this information may be stored or may pass through:

- **Smartphone**
- **Laptop/desktop PC**
- **USB stick**
- **Within a business application** (HR, CRM, accounting, etc.)
- **Backend systems** (e.g., storage, server)
- **Email**
- **Point-of-sale terminal**
- **Public cloud**
- **Accessed via WiFi**
- **Accessed via network**

Next, rank your first list of information by how valuable each item is to your business. Pick your top 3, for example, then find all the places where that information is located from your second list. You could apply simple scoring to this process (e.g., give each item in the first list a rating out of four based on criticality of information and give the second list scores out of four, based on the likelihood that it may be a target for attack). **You have now identified the top areas and resources of your business to protect**.

The table below is a basic template that will help you decide where to invest your security budget and how to spend it most wisely. In later sections of this guide we'll help you fill out the other columns in the table such as the defences that need to be put in place. For the moment, focus on the first two columns labeled Data Assets and Where Data Is Accessed.

Basics of Security Risk

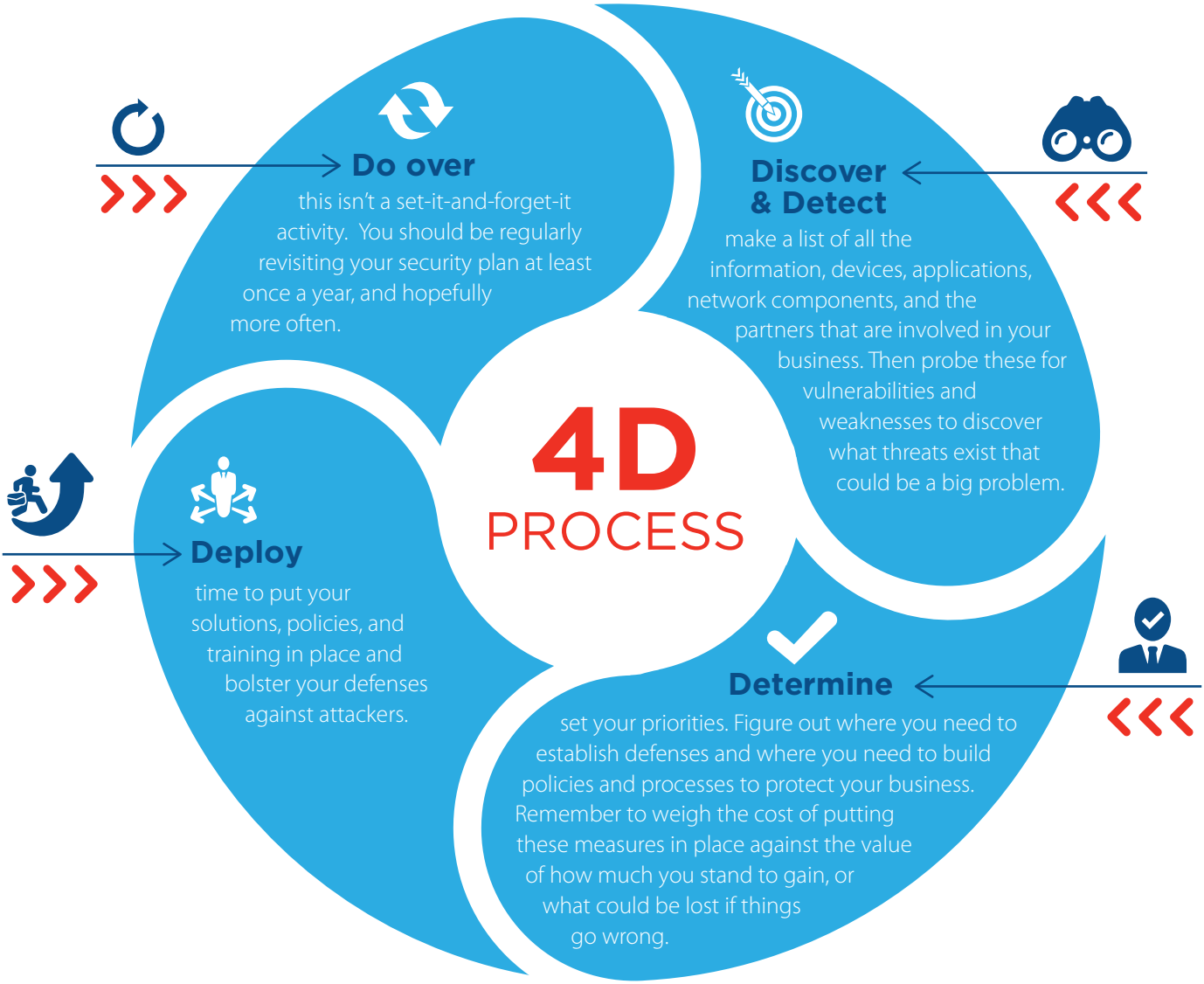
	Description	Examples
Data assets	Data or other valuables that need protecting	Financials, HR records, Customer data, Company process and other secrets, Email messages, Office productivity documents
Where the data is accessed	Where the data is stored and accessed	Smartphone, Laptop/desktop PC, USB stick, Business app (HR, CRM, accounting, etc.), Backend systems (e.g., storage, server), Email server, Point-of-sale terminal, Public cloud, WiFi, Wired network
Vulnerability	Weakness that allows an attacker to get at the asset	Smartphone not updated, Unattended PC, No backup, Employee lack of knowledge, Bad click, Unsecured WiFi, Poor password
Threat	How the attacker uses the vulnerability to get at the asset	Social, engineering, DDoS, Malware, Buffer overflow, Sniffer, Password attack, Physical theft
Source	Who the attacker is	Competitor, Disgruntled employee, Uninformed employee, Script kiddie, Organized crime
Defence	Technology, services and training used to reduce vulnerabilities and block threats to protect assets	Training, Update PC, Back up data, Lock devices, Know good from bad links, email hygiene

Is There a Simple Approach to Assessing Risk?

Planning ahead is the key to beating cyberattackers at their own game. It starts with the basics of security risk management. The process is not complicated, but does take a little time. Most Canadian organizations take a hit-and-miss approach to security planning, guessing at what they'll need or spending to address the problems that have already appeared.

Going through the above exercises assesses what things are most important to your business, and which are lower priorities. You'll be asking yourself questions like: How would my business be impacted if this system went offline? What would be the result if data were stolen? From there, you need to think about how likely it is that these situations may actually occur. A smartphone is easy enough to lose, but an encrypted server locked away behind a steel door is not likely to go missing.

Easy-to-remember guideline for developing a security risk plan can be seen in IDC Canada's "4D" process:



Following this 4D process helps to more precisely determine what should be your appropriate budget for security. In this part of the process, you'll have determined what elements of security are "must-haves" versus what other elements are nice-to-have. You'll price out technologies, labour and/or services to see how these match up with your requirements and your wish list. You'll set aside the solutions that may be too expensive for your needs today, but perhaps make a plan for your team to put them in place at a later point. To confirm if you're in the right ballpark, you can check back to see if your security budget is still approximately 10% of your total IT budget.

Chapter 7
How Much Should My Business Spend on Security?

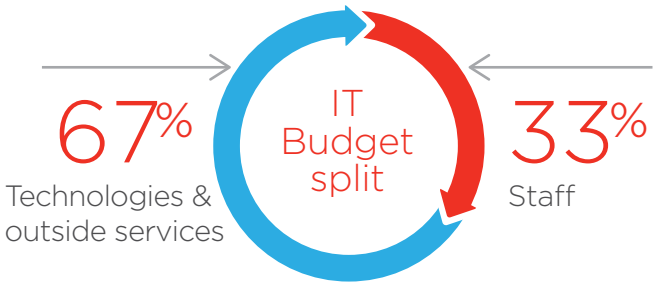
Many small and medium-sized organizations don't spend the appropriate amount on IT security – nor are they spending it effectively. While some organizations may underspend on IT security, which can result in more breaches, others overspend. In some cases, a larger security budget doesn't actually equate to better security. While the dollar amount allocated to an IT security budget is important, it's how that money is spent (different technologies, staff training, monitoring services, etc.) that really matters and has a much greater impact on how secure an organization is.

As a rule of thumb, consider taking 10% of what you would allocate for your IT budget and direct that toward your IT security efforts. IDC calculates that the average Canadian security budget is 9.8% of IT budget and that includes the cost of staff, technology and external third-party services. Because every organization is unique in terms of number of employees, amount of customer information, compliance requirements, connected devices and most importantly risk tolerance, IT security budgets typically vary. You should aim for a budget as near as possible to this recommended average.

Average Security Budget

The average Canadian security budget is

9.8% of IT budget



Among the goals of adopting the 5 Habits of Highly Secure Organizations is that every organization needs to identify the best and most important places to spend limited IT security dollars. Habit 1 (see Chapter 6 for details) identifies areas of your organization that should be highest priority to defend. Doing so determines how your IT security budget should be sliced up in order to effectively protect the most critical information within your organization. The remaining habits focus on the technologies, services, training and recovery methods required to cost-effectively secure your business.

Annual Security Budget Allocation Across the 5 Habits

As a rough guide, here is by percentage the recommended amount of your IT security budget that should be allocated to each of the five habits.

*Depending on the size of a breach this percentage allocation could fluctuate

Things to consider with your security budget:

Prepare & Plan

Prepare & Plan to assess risk – The small amount of budget we recommend for this effort shouldn't lead you to think it is less important. Doing a thorough job in this area helps ensure appropriate spending on all other security efforts. If you have compliance and auditing expenditures (e.g., for PCI planning and auditing) these come out of this line item.

Decide & Deploy

Decide & Deploy technologies and services – Technology solutions and services deployed to protect your smartphones, servers and other parts of your business account for this large allocation.

Test & Train

Train & Test employee security knowledge – In a similar manner to the low budget allocation of "plan and prepare," training employees is not costly. In fact, the biggest bang-for-buck ratio in IT security spending may exist with your investment in training staff who represent your best line of defence. Training is not necessarily expensive, but it does require an investment of time.

Monitor & Maintain

Monitor & Maintain effective threat protection – Your staff and/or an outside provider must keep a watchful eye on your IT security technology and training. Attackers constantly change their methods and security solutions quickly become out of date over time. You must always be monitoring for new threats, while maintaining the integrity of your existing IT environment and continually upgrading employee security knowledge.

Recover & Respond

Recover & Respond – Breaches occur constantly and appear in all sizes – large and small, and everything in between. There's a cost to clean up and repair the aftermath of an IT security intrusion. Larger breaches involving personally identifiable information of customers or employees cost much more to recover from, for example. Expect to spend more if a high-impact breach occurs. Your planning for incident response also comes out of this slice of your security budget.

Chapter 8

Where to Start?

The first step in implementing IT security for many organizations starts with decisions regarding tools and technologies to use. While this is a critical step in fending off cyberattacks and mitigating threats, moving immediately to acquiring tools and technologies is premature. The path to improved security should begin with preparation and planning to assess risk and vulnerability. Before buying security products and services – and prior to launching into this chapter – you need to first identify what needs to be protected by reviewing Chapter 6: "What Parts of My Business Are Most at Risk?"

"Decide and deploy" is all about assessing which security solutions should be used at your organization. It is the next step after you've identified the resources and data most at risk and after you've allocated a budget. At this stage, it's important to understand how attackers attempt to disrupt or outright steal from your organization.

How Hackers Get In

In some cases, an attacker knows the data they want and where it is located and stored. They use software tools of their trade to scan the internet for vulnerabilities – essentially flaws in your software and devices. Or they might use mass emails to find ways of duping (known as phishing) your employees. Staff are tricked by the attacker to give up valuable data.

A successful cyberattack requires these steps:

	Scan the internet	Scam employees
1 STEP	Scan the internet for devices and software that aren't fully secured, patched or updated. This includes networks, smartphones, PCs, cloud applications, websites and many other points for an attack.	Send out millions of malicious files via email. Send millions of emails pretending to be a recognized brand. Hack a website and create fake links which would be clicked on by employees.
2 STEP	Gain access into that device, network or website through an unsecured weakness.	Trick the employee to take an action such as opening a malicious file, clicking on a fake link or giving up a username/password.
3 STEP	Snoop around to see if there's data worth copying or systems worth disrupting.	Wait for an unsuspecting employee to enter data that could have value or might be used to break into other systems.
4 STEP	Copy data and sell it. Disrupt a website, server or network so that it can't function properly.	Copy data and sell it. Disrupt the work of employees by destroying files.

Security solutions and technologies are designed to block each move an attacker makes against your systems or employees. By taking an overall view of where your sensitive data is located across your smartphones, email, PCs, cloud services and anywhere else, you'll begin to form your own guide of which security solutions you need. But you'll need multiple layers of security defences in place to provide effective protection. This is called a "defence in-depth" layered approach to security – and it helps you cover all the bases. It's like having a deadbolt on your front door, locks on windows, maybe an alarm system or even the barking of the family dog to stop an intruder in different ways. If you don't have the right mix of security solutions in place, hackers can watch your activity (entering passwords, banking information, customer data, confidential employee information, etc.) for as long as they wish. Sometimes they make their presence known by holding your data for ransom or otherwise corrupting it. But most often an intruder may look to gain access to smartphones and servers with as little sign as possible they were ever there.

It's impractical to identify every software flaw or to recognize every threat that could result in a successful attack from a malicious outsider. Top software brands themselves offer a "bug bounty" that rewards outside hackers and developers able to identify new vulnerabilities. Even large security vendors know threats change rapidly and new weaknesses that can be exploited continually appear.

It means you need to focus on areas that must be protected and close the potential vulnerabilities that may allow access to your data. In security circles, it's called the attack surface. Just as the doors and windows of a house are vulnerable entry points to burglars, these can be described as a home's attack surface. Of course, it is much more complicated to map out an organization's attack surface because:

- There may be many more points of entry an attacker can use to extract your data (PCs, smartphones, servers, cloud, employees, networks and so forth).

- Your attack surface constantly changes and expands. For example, the simple act of sending an email with confidential information to a customer expands your attack surface to now include the recipient's inbox.

To protect against unwanted exposure, changes, sharing or potential compromise and destruction of your business's important data, you need to defend the following 10 areas:

Employees

The greatest risk for data being exposed among Canadian organizations is through the actions of employees who, knowingly or not, behave in ways that increase risk exposure. Many IT security risks and data compromises are a result of employee behaviour – like using the same password for multiple applications, not regularly updating applications and operating systems on a smartphone and PC to the latest versions, clicking on high-risk web links, getting phished by a seemingly reputable email that is in fact fraudulent, or otherwise improperly sending out confidential company information.

Files and data

This is the greatest prize most attackers seek. Attackers use weaknesses found in your attack surface to gain access. Smartphones, USB keys, disk drives and even printers provide entry points to confidential files and data. These can also be part of an attack surface as well and not just the target. Each of the other nine areas of your attack surface are means by which an attacker aims to expose coveted data. There is only one way to directly protect the data itself, and that's by encrypting it. Many smartphones come prepackaged with encryption turned on and many websites now use Secure Sockets Layer (SSL) encryption to ensure your banking and other transactions are safe. There are situations where company email and other applications may not have encryption switched on or even be capable of it. Solutions such as virtual private networks (VPNs) can handle these cases, however.

Applications and operating systems

Attackers continue to find new flaws and ways to exploit weak software coding in order to alter the way the application is intended to run – or to gain access to the files accessed by that application. Ensuring applications and operating systems are always current and upgraded to the latest versions, by downloading and installing updates as soon as they come out, is a simple yet effective way to reduce the risk of a malicious attack.

Browser and web usage

Because the browser is the way employees access websites, the simplest security solution comes down to training employees on basic "dos" and "don'ts" regarding which links not to click and how to avoid drive-by attacks (e.g., accidentally downloading a virus by clicking what looks like a legitimate pop-up window in a browser). Company-wide solutions can be deployed too that restrict access to known malicious websites and help defend against phishing and drive-by attacks. Other solutions are available that ensure confidential user traffic is encrypted while using public WiFi or when the data is passing over the internet. Try to avoid adding excess third-party plugins, such as ad blockers, stock tickers, weather updates or anything you download and install for your browser. They can introduce all sorts of vulnerabilities that can be exploited by an attacker. Please note that many recognizable brand name plugins are more rigorously tested for security – and can be helpful – such as certain password managers.

Email

Thankfully, most spam has been reduced to a minor nuisance. As email continues to migrate to the cloud, more and more basic security is delivered through a service provider (sometimes for extra fees). Today, email security is delivered through antimalware protection (e.g., scanning attachments for viruses), antiphishing (e.g., blocking or otherwise disabling suspicious email content and links), encryption (e.g., ensuring a message can't be read while it travels across the internet) and employee training on best practices.

Web server

Above we outlined secure web surfing habits. Many organizations also run their own websites – and these need to be secured separately. Attackers can harm your website in a number of ways including reducing customers' ability to access it, stealing valuable data from it or possibly defacing it. Web security is a top issue when the website is used to collect customer data or store other sensitive information. Web servers, databases and application software that are online can be easily compromised and are a top target of hackers looking for valuable information. A web server must be correctly configured by a professional and software must always be current, otherwise you run the risk of exposing online resources to serious attack.

Cloud

IT security in the cloud is a shared responsibility between service provider and customer. When using the services of a cloud provider, you need to understand where their IT security capabilities begin and end. For example, how might a service provider respond to a security incident, breach or data exposure? Public cloud providers have limits and typically offer only some security services while leaving others to be managed by the customer. The reasons for this are practical – a cloud provider may not know when an employee leaves your organization and would not be aware that login privileges must be revoked. Your company needs to be managing accesses and privileges. Also, a cloud provider may not know which of your data is highly confidential and shouldn't be shared by employees (customer data, certain financial data, etc.). Also, note that data stored in the cloud can be impacted by a ransomware attack if an employee accidently launches certain malware, for example.

PCs and smartphones

Smartphones, PCs and other connected devices hold valuable data that can be compromised. These devices are also entry points into your network and other data sources within your organization. Lost devices or vulnerabilities within a device or application give an attacker an opportunity to gain control. PCs and smartphones are often called "endpoints" by security experts – you'll hear about solutions such as "next-gen endpoint" to help protect devices. An often overlooked and effective security defence for devices is to simply do regular backups. Back up your devices and have a "bootable" copy (e.g., all apps and data you need to get up and running fast is backed up) for a quick restore if you're the victim of an attack or lost device (e.g., ransomware won't work on you if you have backups).

Servers

Like PCs and smartphones, servers are potentially vulnerable connection points to the network and often contain much more data. Similar to a PC, security software should be installed on servers to ensure only authorized staff have access. Likewise, you'll want to ensure application and operating systems are up to date and backed up regularly. Even if you run servers in the cloud, the same security practices hold true.

Network

As the pathway for all traffic between your applications and devices, securing wireless and wired networks is a foundation of your IT security defences. Because files and data are in constant flow – and often don't stay within the confines of a single network – cybersecurity needs to extend across the wider internet and be used to protect your data wherever it is while being transported. An important concept of network security is called "segmentation" or the notion of separating your network into high- and lower-risk areas. The solutions used to protect each network segment depend on the amount of sensitive data or critical applications connected to it.

Chapter 9

Which Tools and Technologies Are Most Important?

What's been previously explained maps out a sort of battlefield of your attack surface. Now it's time to deploy the troops. Similar to a military commander, you'll need to use a range of defences to protect your domain. In the context of your business and its IT security, that means deploying technology and monitoring/management services to block attackers and alert you to their presence and activity.

Below is a cheat sheet with a list of basic security solutions to consider as part of an arsenal to defend the many points of weakness that may exist across an organization. You'll notice there is no single solution that secures any one area of an attack surface, with a single exception – employee training. Many of the other listed solutions also help ensure employees don't accidentally or intentionally put your business at major risk by weakening IT security. But to block the paths an attacker might take to access your data, you'll need multiple layers of IT security.

Security Solutions to Defend 10 Critical Areas of Your Attack Surface

Attack surface	Security solution
Employee	Training
Files & data	Encryption ▸ data loss prevention ▸ backup
Applications & OS	Password manager ▸ apply updates/patches ▸ vulnerability scanning*
Browser & web usage	Train employees ▸ apply updates/patches ▸ limit use/disable plugins
Email	Antimalware ▸ encryption ▸ anti-phishing ▸ anti-spam ▸ strong password
Web server	Antimalware ▸ vulnerability scans* ▸ web app firewall ▸ code testing ▸ DDoS protection
Cloud	SaaS: ▸ encryption ▸ data loss prevention ▸ account provisioning, PaaS/IaaS: ▸ Password managers ▸ defenses for SaaS ▸ plus all the other network ▸ application and web defenses
PC/smartphones	Antimalware ▸ data loss prevention ▸ backup ▸ strong password ▸ remote wipe ▸ enable encryption ▸ two-factor authentication
Server	Antimalware ▸ firewall ▸ vulnerability scan* ▸ password manager
Network	Firewall ▸ intrusion detection ▸ log management ▸ security information event management(SIEM) ▸ segmentation ▸ DDoS protection

*A vulnerability scan can be supplemented by or in some cases replaced by penetration testing that an outside security provider can run for you.

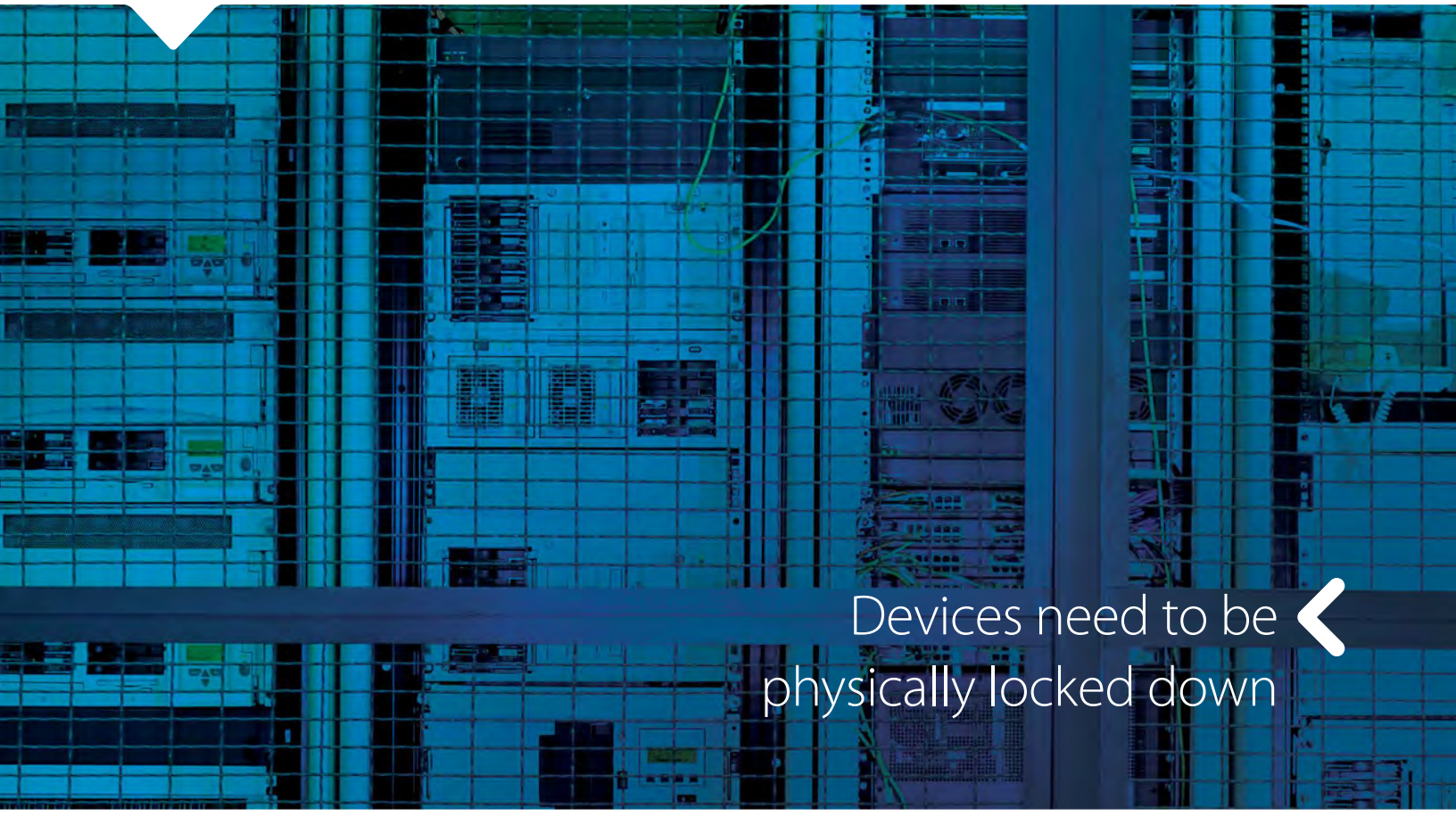
See the glossary at the end of this handbook for a definition of these terms.

Unfortunately, there is no single security appliance or application that addresses the complete range of defences outlined above. As outlined earlier in this section, your organization needs to take a layered (also called "defence-in-depth") approach to security protection. You'll need staff expertise or the services of a trusted advisor to develop a holistic security environment for your business.

Also, once a firewall or other solutions are deployed they will lose their ability to secure your organization over time. Vendors will typically provide updates to their solutions to help you maintain a high level of protection while you own their product. But in security just like with all other software and hardware, upgrades are required every few years (e.g., if you want the solutions to be constructed with the latest threats in mind). Attackers' methods change continuously, so you'll need continual monitoring and management – either by internal security staff or through an outside managed security services provider.

Remember Physical Security

Physical security is quite literally about securing the physical smartphone, server, PC, USB drive and any other physical storage that holds valuable data or could be used by an attacker to gain access to your network and other sensitive data. Devices need to be physically locked down as much as possible. When an attacker gains direct access to your systems, it's an opportunity to launch attacks that wouldn't otherwise be possible. For instance, they might install a device that is able to store valuable information as it passes through the system. An example of that might be an attacker that has been able to alter a physical credit-card-reader terminal, which we see the result of when your credit card company calls to inform you that your card was compromised.



Chapter 10

What Should an Employee Training Program Include?

IDC believes Canadian organizations need to provide more training for staff on the basics of good security practices. Doing so is neither difficult nor costly. In fact, training can cost as little as 1% of a security budget. By conducting lunch and learn sessions, sending out best practice email reminders, providing links to YouTube or other security content, a lot is accomplished with few dollars expended.

Staff security training should be considered your first line of defence against attackers. Attackers count on and succeed when your staff aren't informed or have lapses in their security habits, such as using the same password for multiple business and personal accounts.

Plan on training your employees in best cybersecurity practices right from the day they are hired. Canada's privacy commissioner recommends taking this step in your hiring process seriously. You may want to commit new employees to adhering to your security policies and understanding their importance by having them sign a contract stating they will follow your guidelines.

Training should be refreshed annually during a formal session to ensure employees have the most up-to-date knowledge. Beyond that, you should look to reinforce the importance of protecting the company's data and assets in regular meetings and conversations. When it comes to what you should train your employees on, consider who, what, how, when and why.

When it comes to what you should train your employees on, consider ***who, what, how, when*** *and* ***why***.

Who should be allowed to access systems and information at your company?

What are they allowed to use business computers and devices for — and perhaps more importantly, what are they not allowed to use them for? What does a suspicious email or website look like?

How are they expected to treat sensitive customer or employee information? How should they use a password-management tool?

When an emergency security situation arises, what should they do?

Why it's critical for your business to follow these policies, including the potential negative outcomes for the business and themselves if they're not met?

A simple start to security training subject matter is to tackle passwords first. Passwords are a means to securely access a wide variety of business applications, systems and confidential information. Yet there are many common mistakes people make with password security.

The Government of Canada has identified a few best practices:

- Don't use the same passwords to access multiple services, apps or systems. The first thing a hacker will try when they scoop one password is to use it on other systems.
- Use more complex character combinations and not ones that are easy to guess. Conventional wisdom says to use at least one uppercase letter, one number and one special character (e.g., B@tM3n11). IDC recommends getting employees to use long passphrases that they can recall – as opposed to random strings of characters, which are nearly impossible to keep in mind. Employees might use phrases containing several words, or even acronyms of words, that would be hard for others to guess.
- Change the password regularly. This reduces the chance of an account being compromised.
- Never share your passwords with anyone and especially not through email.
- Don't write down passwords. For example, don't make the classic mistake of placing a sticky note with a password on a monitor.

Employees should consider using a password-management application to ensure strong passwords are always selected. The employee needs to remember only one password for the password manager while the application in turn creates far more difficult passwords for other applications and systems, including those that are cloud-based. Password managers are simple to use and widely available.

Phishing – Don't be an Easy Catch

Hackers often use social engineering tactics to penetrate an organization's defences – things like sending an employee a message that looks relevant to them. The message might appear to be from someone legitimate within your organization, or perhaps from a business partner or web service from whom they expect to receive messages.

Attackers will try various social engineering tactics to convince people to click on a fake or malicious link or to download a virus in an attachment. To reduce the success of phishing attempts:

- Keep your operating system, antimalware software and other applications up to date so the impact of any phishing attack damage can be minimized.
- Never click on links contained in emails. If someone sends you an email with a link, be suspicious. Even what may look like a familiar website link could in fact be something more sinister.
- Don't trust email attachments. Make sure your email application doesn't auto-download attachments and that your antivirus scanner is actively scanning attachments before they are downloaded.

Another related technique to phishing is called a **drive-by download**. Instead of taking the form of an email or social media message, this attack often comes in the form of a clever pop-up contained within a web browser, seeding search results with infected links or finding a way to embed a malicious file on a trusted website. Train your employees to be extremely cautious of pop-up windows. The best practice is to have your web browser block all pop-ups by default, and then temporarily turn off that block on a trusted site.

Social media, too, has become a far more common place where attackers try to lure in unsuspecting employees. Through services like Twitter and Facebook, they create a false identity so that a message sent to an unsuspecting employee appears as though it legitimately comes from another internal employee, such as an executive. Getting a list of who works at a company is extremely simple online today. Any social network where employees can receive messages are a point of risk.

Getting Started With Employee Training

To help employees adopt the correct security behaviour you should:

- Ensure staff understand what organizational information is essential to protect. They should be identifying it in their own daily work. Guide them on how to use that information correctly and how to protect it. Ensure they are aware of the legal implications for the business when privacy best practices are not followed.
- Require that staff regularly change passwords – every 60 to 90 days is typical.
- Encourage them to use passphrases if this is an option within the applications and cloud services they use. These are easy-to-remember plain language phrases such as the "Blue horse hopped a train to the clouds." This is preferred over using hard-to-recall passwords that require a mix of capitals, letters, numbers and special-character symbols. Better yet, encourage employees to use a password-manager tool.
- Have them use two-factor authentication where possible (e.g., require a second login step to identify themselves, such as a swipe card or a fingerprint scan, which are becoming a typical feature of smartphones and PCs).
- Teach staff to recognize phishing emails and how to avoid the traps of social engineering. They should never respond to an email that asks for confidential information such as a password, or click on a link sent in an email. IDC has seen attackers successfully trick a Canadian organization into making financial transactions to what they believed was a known supplier. Accounting, HR and all staff need to be vigilant.
- Explain the importance of keeping applications and operating systems current as soon as the alert to an update appears on their smartphone or PC.
- Keep staff fully aware of business security policies.

Earlier in this guide we talked about advancing the security maturity of your business. We also discussed an 18-month plan to help your business progress toward its security goals. If you're moving along that road and feel you're ready for the next step in training, you might want to consider some table-top exercises. These are security drills that simulate an incident and attempt to evaluate how well staff apply their training. These drills also help you to discover potential weaknesses or gaps in plans and policies. It may be useful to enlist outside help from a cybersecurity expert to run these sorts of exercises. Software packages are available for purchase that help rollout an employee security testing program. For example, emails are sent out with a fake link to assess how many employees click on it. Other various phishing techniques can be used too. This will demonstrate to employees where they may have strayed from their training. Some organizations run these simulations prior to training employees in security in order to benchmark levels of knowledge and encourage employees to pay full attention during security training sessions.

How to Sell Security to Your Staff?

It's easy to end up in a place where your employees bemoan cybersecurity efforts. IT departments are often seen as wagging the finger and shutting the door on potential business opportunities all in the name of IT security – or simply being an added nuisance. If this happens, your security efforts are likely to fail because employees view these policies as obstacles to doing their work.

Build employee support for security policies by sticking to a few guiding principles:

- **Keep it simple** – Don't create a thick binder of complicated rules and policies for your employees to read and follow. Asking staff to read something longer than a couple of pages may be overwhelming. Instead, provide condensed guidelines in the form of a few core concepts written and expressed in simple, plain language. Reinforce the written message through a workshop or interactive session.
- **Choose your battles** - Prioritize your security approach to focus on the high-risk areas that have the greatest impact on your business. IDC recommends beginning with instruction on how to identify a phishing scam or how to use a password manager (using a password manager eliminates the issue of reused passwords).
- **Get buy-in** – An effective security policy is fully dependent on the commitment of the people in your organization – before it's created. Policy creation should not live exclusively with some security expert. By involving staff in the creation of policy you're more likely to get their buy-in, especially early on. Staff can identify data that shouldn't fall into the wrong hands. They might also consider the various ways data could be exposed. Building a policy together with your employees encourages them to own and commit to it. It also helps educate them on how to behave and act more securely.

Chapter 11

How to Identify an Intruder?

Sometimes a security breach is as obvious as opening up the vault to find a ski-mask-wearing thief shoveling money into a burlap sack. For example, a laptop is locked out with a clear ransomware notice glaring at you demanding money. But more often than not, it won't be clear that a device or system has been breached at all.

A cyberattack isn't a "smash and grab" operation. Rather it's a "stay and prey" ongoing activity. Attackers establish a foothold in a system and wait patiently to discover and exploit a vulnerability that might eventually allow them access to the most valuable information in your organization and to capturing new data as it's being stored. Many well-known breaches were only discovered months or even years after taking place.

An intrusion simply means that someone you don't want to gain access to your data is actively attempting to break in to your network, smartphone and other devices or has already gotten in. It's the type of thing that you need to be aware of and alerted to quickly if and when it happens. Use available tools and services that can alert you to an intruder.

You need to focus on the fourth habit of continuous monitoring and maintaining network and device security to proactively defending against new threats before they become breaches. Cybersecurity defence needs to continually evolve. Additionally, the defences you put in place, such as your firewalls or data loss prevention solutions, become less effective over time. They need to be tuned to make sure they're not flagging too many things that aren't actually breaches – or worse, missing a breach.

Tools and Services to Detect an Intruder

The good news is that monitoring solutions and managed security services are better than ever in their ability to contain and eradicate an intrusion when it happens. Readily available solutions now use sophisticated analytics (essentially the same sort of artificial intelligence used in self-driving cars applied to security) to detect intrusions at the earliest stage. Thankfully, you and your staff don't need to be fluent in the terms and techniques of Big Data analysis. The solutions themselves take care of it for you.

Here are **three common and effective tools** you should deploy – either managing them yourself or using the services of an outside provider:

- **Intrusion detection and prevention (IDP)** – These tools flag unusual and potentially harmful activity on a network. Essentially, you or your provider puts an IDP software or a hardware appliance on your network to watch for suspicious traffic – and block it if need be.
- **Security information event management (SIEM)** – SIEM technology watches over all the activity across different devices on the network to provide early warning signs of an attack anywhere on your attack surface. Many midmarket or larger Canadian organizations with a bigger network and dozens if not hundreds or thousands of servers typically use these solutions.
- **Threat intelligence** – Threat intelligence services look outward across the globe to determine how new threats are forming and figure out ways of blocking them. This is a feature of managed services and increasingly some firewalls and other network defence technologies.

To effectively detect intruders, you need to monitor:

- Devices or servers that are exposed to the internet and any device or system connected to those devices and servers
- Connections to branch offices, partners and remote employees
- Applications dealing with sensitive information accessed via a VPN. A VPN creates a secure virtual tunnel between a remote worker's PC, for example, and company applications
- Places where critical company information is stored

Chapter 12

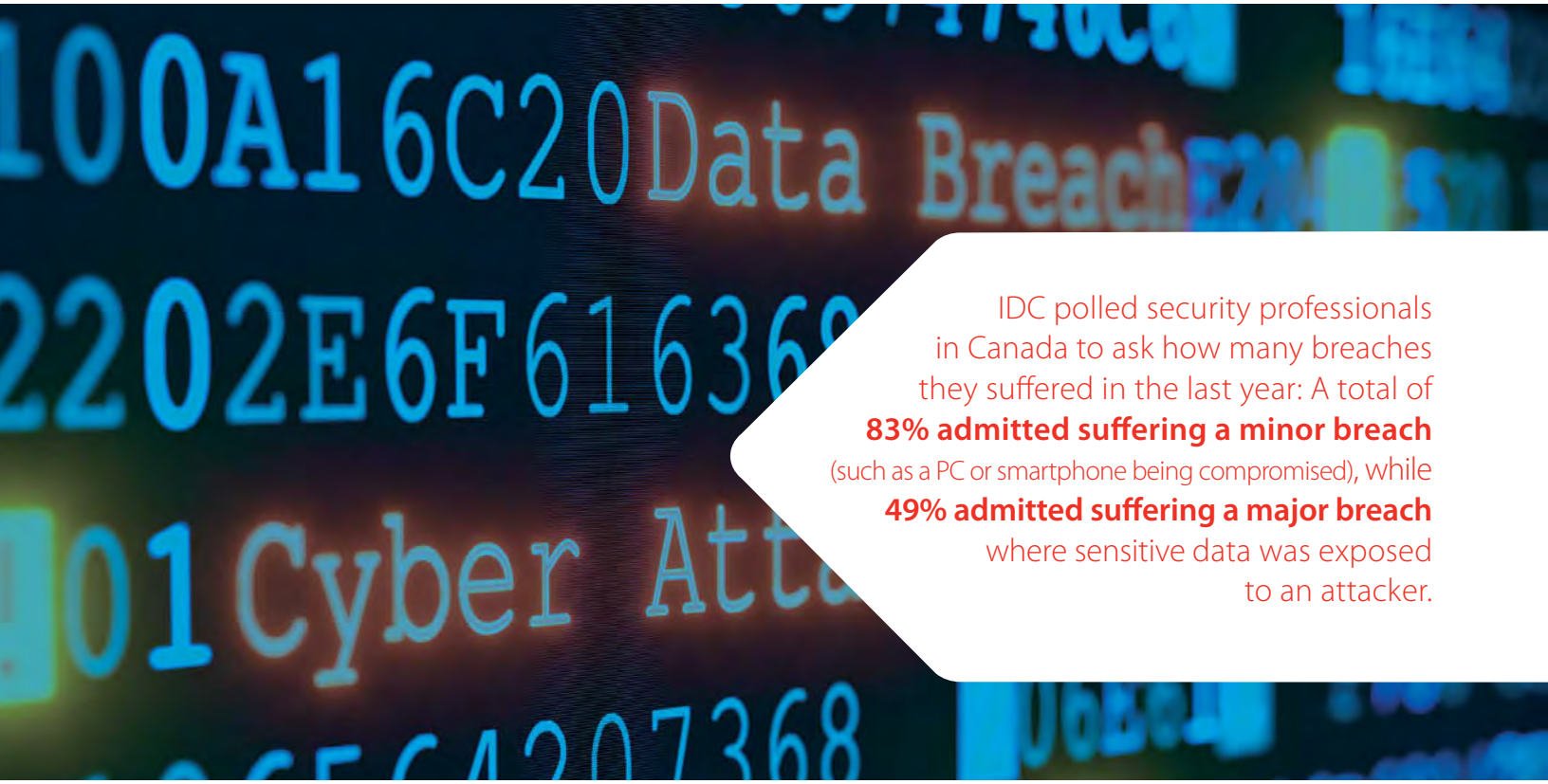
What to Do During and After an Attack?

There's an old saying among security professionals – it's never a matter of IF you get breached, it's a matter of WHEN. Despite doing everything you can to prevent breaches, it's inevitable that your company or organization will be subjected to an attack and perhaps an intrusion. So you need to understand how to prepare – to mitigate attacks, minimize the impact of a breach and recover quickly.

If you worked through the first habit of "prepare and plan" to determine which data is most important to your organization and where it is located, you are in a good position to plan for inevitable security incidents. With proper defences in place, based on the direction provided in the second habit ("decide and deploy"), you're in a position to reduce the risk of a breach occurring in the first place. Defences are further shored up with employee security training as described in the third habit. And, by executing on habit four of monitoring your defences, your organization has increased its ability to block threats and adjust as attackers move to change their tactics. The fifth and final habit of "respond and recover" focuses on quickly resolving a breach with as little stress and disruption to your business as possible.

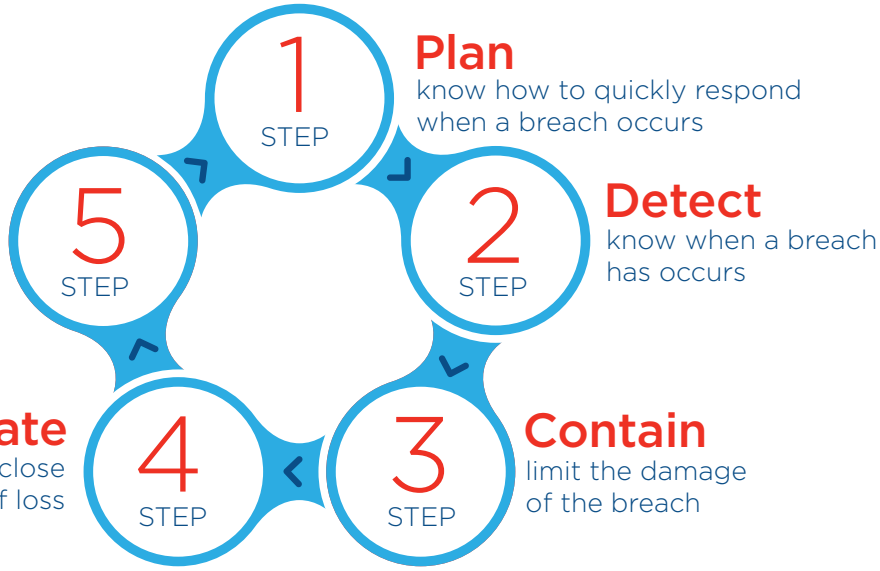
A security incident may take several forms. Perhaps it's an unauthorized person accessing a server, or a malware attack on a smartphone. It could be a denial of service attack targeting your website, applications behaving in unusual ways, or it could simply be a laptop that is lost or stolen.

Regardless of what security or threat situation your business faces, you should have a plan that allows your business to continue serving customers even in a worst-case scenario. Incident response planning is a way to continue operations despite disruptions. Unfortunately, IDC research shows almost half of small to midsize businesses either don't have a plan or take an ad hoc approach when security incidents occur.



IDC polled security professionals in Canada to ask how many breaches they suffered in the last year: A total of **83% admitted suffering a minor breach** (such as a PC or smartphone being compromised), while **49% admitted suffering a major breach** where sensitive data was exposed to an attacker.

Five Steps to Rapid Incident Response



Step 1: Plan

Identify who reacts first, leads and owns the initial response to an incident. Identify which team members need to be pulled in, how and what to communicate to impacted employees and customers, and what needs to be documented. Most importantly, determine what takes priority based on the severity of the incident. A minor, low-priority incident might only impact one or a few employees and their IT equipment such as a PC, for example. A medium-level incident might be a server that has been taken offline. A major, high-priority incident may be one where sensitive data such as personally identifiable information has been exposed.

Step 2: Detect

Sometimes it will be obvious when a breach has occurred, such as a PC or server that goes offline or a ransomware note appearing on an employee's screen. In other cases, you might not know unless you have followed the fourth habit of monitor and maintain (explained in the previous section) by putting technology or managed services in place to continually monitor your attack surface for nefarious activity.

Step 3: Contain

The goal here isn't just switching off IT equipment and yanking out the network cables. It's to keep the IT resources available to legitimate users while blocking out the attackers. Once a breach is detected, you'll want to involve multiple stakeholders - the user(s) of the IT resource, any partners that provide security or internet service, and the staff responsible for that hardware at your company. React quickly, but at the same time make sure someone with the appropriate skills is addressing the problem – you don't want to end up doing more damage. Use your security tools and solutions such as firewalls, network controls and other available means to isolate affected devices.

Step 4: Eradicate

Once you've gained control of your systems or devices again, it's time to wipe out the effects of the attack and board up the entry point where it came in. You need to use security solutions to scan and clean devices of malware or other threats. If necessary, rely on backups to restore systems to an earlier, trusted version. Those that are more security-savvy and advanced will look to create an "image" of the breached and/or compromised systems to study for forensic purposes.

Step 5: Recover

With your devices cleared of any ill effects and infections, you can return these to operation and use. Test these systems for reliability and then send it back to work. You'll want to keep a close eye on performance. Then it's back to that good monitoring habit with a higher priority for tasks like watching accounts, services and traffic to and from affected systems and devices.

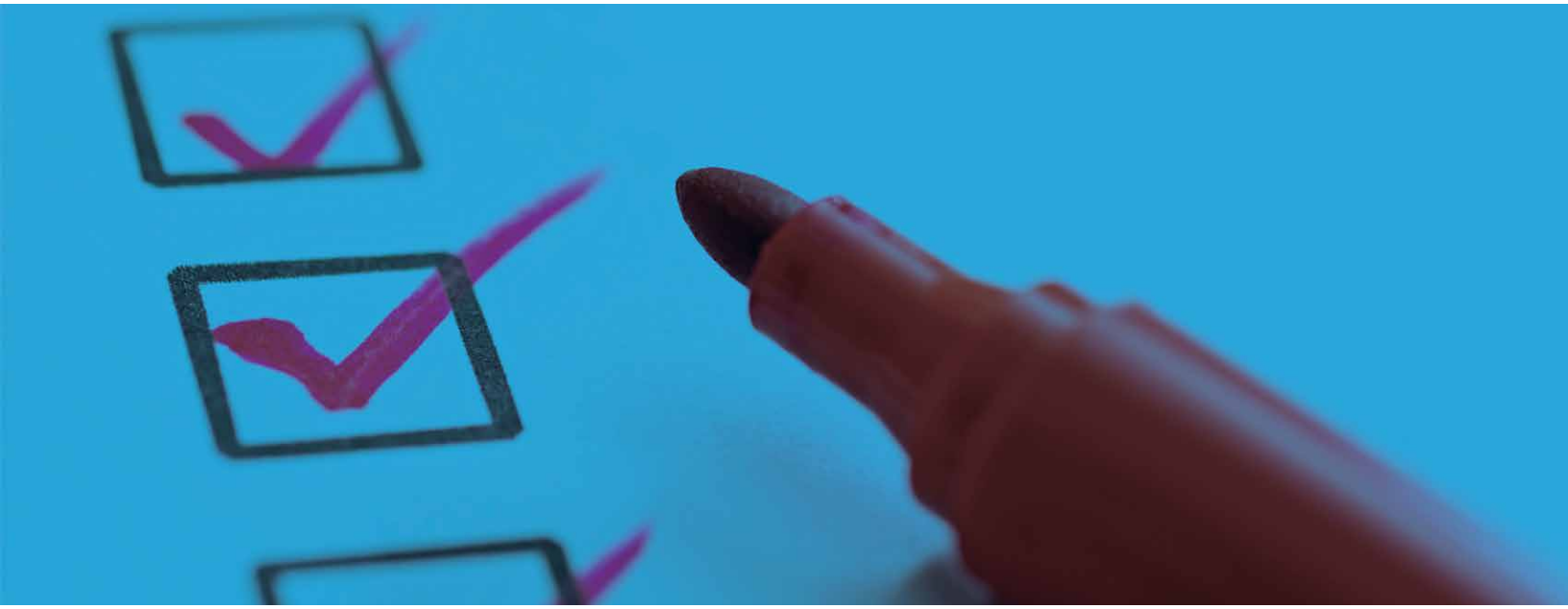
It's advised that you seek outside professional assistance when creating an incident response plan. If there is a criminal aspect to an incident or if legal counsel must be brought in for exposed personally identifiable information, then you need to follow and document a well-thought-out plan.

Here's a checklist of what to document and assess when a breach is detected:

- ☑ Name and contact information of the person who detected the incident for any follow-up information
- ☑ Physical location and network information of the breached system(s)
- ☑ The types of data stored on the breached system
- ☑ Specify if certain files contained personal information and indicate their size and location
- ☑ Level of encryption used on the data
- ☑ Description of how many employees and customers are affected
- ☑ Description of the current state of the system (on/off, connected to the network or not, etc.)
- ☑ A plan for contacting customers if personal information has been exposed. Message out to them as quickly as possible to get ahead of potential backlash

After you've recovered from a security breach, a post-mortem meeting should be held to discuss things like what happened, why it happened, how the organization responded and what was learned as a result. It's not a finger-pointing exercise to assign blame. Instead, ask questions about your security plan and how it and your response can be improved. Are different solutions and controls required? Is better training required for staff? Document employee recommendations and consider if there is a business case for enhancing security solutions or training.

Also at this point you may need to notify customers or employees, particularly if they've had their personal information compromised as a result of the breach. As previously mentioned in the section on privacy and compliance, your company may be legally required to disclose this information in a timely manner.



Chapter 13

Why Should Your Business Find its Security Maturity?

Your business wasn't built in a day and your security defences (sometimes called your security posture) will likewise take time to develop. Creating a mature cybersecurity posture is multifaceted. There is no single or simple solution that will make an organization secure. It does require effort, but IDC research concludes that those organizations with a higher level of security maturity experience far fewer breaches. Planning pays off.

A higher level of security maturity is attained by committing to sound practices rather than an ad hoc approach of simply spending more money (assuming your security spend is in the recommended range of 10% of your total IT budget). IDC finds that solely increasing the amount you spend on security is usually not the answer, particularly if it is not spent in the right places. Achieving a higher maturity level is a matter of planning and training – and that doesn't need to be expensive.

IDC examined the security approaches and practices of hundreds of Canadian organizations and developed a concise outline for what actions your organization should take to improve security maturity. The most secure Canadian organizations focus on security training, security risk planning and security technologies.

Security Maturity Progression

Level 1 **Basic**

Result

- Highest number or breaches
- Under spend on security

Approach

- Basic security - ad hoc without a strategic focus

Level 2 **Technology** centric

Result

- Highest number or breaches
- Over spend on security

Approach

- Focused specifically on security **technologies**

Level 3 **Planners**

Result

- Lower number or breaches
- Spend appropriately on security

Approach

- Focused on security **technologies** and security **risk** planning

Level 4 **People** centric

Result

- Lower number or breaches
- Spend appropriately on security

Approach

- Focused on security **technologies,** security **risk** planning, and staff **training**

Small and medium-sized businesses are typically not as secure as larger organizations, due in large part to inadequate budgeting and effort allocations. For example, IDC research shows that smaller organizations typically spend additional security funding on technology rather than employee training. As has been previously discussed, it's a matter of putting the right effort in the right places.

Training and education provides the greatest "bang for the buck" when it comes to deciding where to invest limited funds.

Consider some of these tips for creating your security strategy:

Leadership

Build a culture of security among staff. Be willing to go beyond "good enough" by allocating budget appropriately to instruct staff on how to protect confidential employee, customer and company data. Have a competent point person at your company who orchestrates a security strategy and is responsible for communicating it to all employees. Ideally this is a professionally trained specialist in cybersecurity, rather than someone simply willing to volunteer for the job. Canadian small businesses identify lack of leadership as a major stumbling block to effective security.

Policy

Create a standardized set of practices to follow that outline how best to respond to and resolve a security incident, and also identify potential security issues. Rather than just reacting to something that might happen, plan strategically and anticipate what could go wrong and how to react accordingly.

Budget

Determine how much money you need to dedicate to security and more importantly where you need to spend it. Consider the value and importance of the business assets you need to protect – and to what degree – in order to assess how best to spend your security budget.

Awareness

Be aware of new threats that continually emerge so your organization can appropriately update its plan, training and technology. You don't need to be a technical expert on the topic, but it's important to be aware of major developments happening in the security space.

It's important to consider the timeframe over which you'll put your plans in motion to advance your security maturity. IDC suggests an 18-month plan as a basic start. The goal is to ensure you are continually improving and expanding your overall protection. Start with a basic assessment that identifies which areas of your business require the most protection.

The assessment forms the basis for a larger security plan. Chapter 6 of this guide explores in more detail how to create a security plan. Once you have a plan, begin regular staff security training, while also putting the right technologies and monitoring in place. And you'll need to create a response plan to react quickly in the event of a breach.

The goal is to ensure you are continually improving and expanding your overall protection.

Draw out a simple plan such as the one below:

Your Security Rollout Calendar

Timeframe	Goals	Security habit addressed
Today	A basic level of security with awareness of security technologies and essential staff "dos" and "don'ts".	Start Habit 1. Habit 2 is already in progress. Habits 3 and 4 should be started at this time
6 months	You follow a plan that seeks to protect the most valuable assets of your company. You have identified the right technologies and know what defences are required. You've started staff security training. You are looking for capable security expertise – whether in-house or delivered by a managed service provider.	Habit 1 is mastered. Habits 2, 3, 4 and 5 need refinement.
12 months	You use an approach that layers multiple security technologies (similar to the layers of protection available on a smartphone such as fingerprint scan, encryption, antimalware, etc.) to deliver the most effective possible protection of critical data and company assets.	You're well on your way to having Habits 1 to 4 in good order. Habit 5 could use a little more work.
18 months	You have applied a highly refined and ongoing measurement of the effectiveness of your security technologies, training, risk planning and incident response. You utilize proactive continuous monitoring.	All habits are being maintained with few problems.

Chapter 14

How Does My Business Maintain Strong Security?

You've learned how attackers work and the many ways they can cause harm to your business. You've learned about the rising occurrence of data breaches and the legal requirements around protecting personal information. You've learned how to defend your business. Now it's time to take what you've learned and put it into action.

Take control of the cybersecurity of your business by taking these measures:

Put Someone in Charge

You need to make clear who leads security for your business. Whether it's yourself or someone else with the right talent, appoint your security leader and announce it to all. Your security lead should be seen as someone with the authority to rally staff and instruct them on necessary security practices. A security leader has technical knowledge and should be an effective communicator. Not only will he or she need to deploy and manage the tools and services required to stay secure, this person must get everyone in the organization to follow security policy.

Particularly in small businesses, one person may need to take on multiple responsibilities, from assessing risk to training employees to maintaining technology. IDC research finds that the average Canadian small business has only half a headcount to handle any and all security requirements. They indicate they need at least one more full-time staff. Similarly, the average midmarket organization has two staff working on security in some manner, but wants to add two more full-time headcount.

Identify Your Biggest Risk and Address It

In Chapter 6 you identified the data most important to your business. Now you must protect it. Map out where it's stored and where it travels across your network and beyond. Remember to reference the attack surface chart in Chapter 9 to help pinpoint what you need to protect. Choose the solutions that you feel will most effectively mitigate your risk. No one security solution or service will provide complete protection. Consider the mix of solutions that layered together defend your smartphones, PCs, servers, cloud services and all other points of weakness.

Determine What Skills You Need

With your solutions identified, you'll need to assess if your staff has the skills and time necessary to deploy, manage and monitor them. Perhaps the security lead you selected has the required technical skills. If your staff lacks security certifications such as the CISSP designation, they may need training. Even if your staff are technically proficient and you feel confident they can do the job, you'll need to identify how to improve professional development to keep up with the changing threat landscape.

- Trusted advisor in your peer group and/or at a service provider/vendor
- Independent media and vendor publications/threat reports
- Standards bodies and government institutions responsible for cybersecurity
- Local security groups
- Security services providers

You're not on your own. Many people in the security industry are working to help organizations like yours (please refer to Chapter 5 for a full list of sources)

Bringing in Reinforcements

If at this point you're thinking you just can't do it all, don't worry. Many businesses are hard-pressed to address cybersecurity with the speed that's required by today's evolving digital landscape. Many small businesses feel they don't have the budget or even enough work to justify hiring a full-time certified security professional. That's where a security consultant or managed security service provider can be a good option. When you hire a service provider, they take on your security problems and work around the clock to solve them.

Train Your Staff

With your security leader appointed and the solutions and services selected and deployed, the next task on your "to do" list is to train staff on good security habits and practices. Take the collaborative and simple approach we discussed earlier (in Chapter 10) and plan the necessary meetings and announcements that will educate your team. Start by educating employees on the social engineering ploys used by attackers. Remember, the people at your company are an attack surface just like your smartphones or your servers. You need to patch up the vulnerability by informing them of the most common tactics.

Training staff and improving the security of your business will seem challenging at times. Remind your staff – and yourself – that not only is protecting personally identifiable information often required by the law, it's the right thing to do. Your customers and your employees have entrusted your business with information that could be used against them. You need to do everything that's reasonably in your power to protect them, or you'll be letting them down.

Keep Your Plans Updated

Your security risk plan identifies the security defences you need and how much you need to spend. But what needs protection and the best way to protect it changes over time. Revisit the plan on an annual basis to keep it up to date. You also need to update your incident response plan. How quickly and effectively your organization reacts to a breach or other security incident is paramount to minimizing the costs when a major or minor incident occurs. Ensure your risk and incident response plans are treated as living documents.

Your business is going to become more digital – and the size of your attack surface will continue to expand. You'll see ever-larger data breaches and hacks reported in news headlines. But many more Canadian organizations will suffer costly breaches that never make the headlines.

Now it's time to take what you've learned and put it into action.

Chapter 15
Glossary

Third-party plugins
There are thousands of software programs called plugins that users can install to extend the capabilities of a web browser. Browsers like Chrome, Firefox and Internet Explorer typically are downloaded with only basic functionality. Plugins such as ad blockers, password managers and bookmark managers can be helpful while using the web. But plugins can also lead to a lower level of security in some cases because either the plugin wasn't coded well or an attacker intentionally created it as a clever exploit.

Account provisioning
This is security software used to manage and control access to IT systems and websites by employees and customers. When a new employee is hired or leaves an organization, account provisioning allows organizations to assign and delete a login username and password.

Account verification
See authentication.

Antimalware
Software that's designed to detect, remediate and prevent active or inactive types of malware including viruses from running on computing devices and systems. Antimalware can erase malware from an infected smartphone, PC, server or other device.

Antivirus software
Software specifically designed to block active or inactive computer viruses and stop them from running. It can erase the virus from an infected smartphone, PC, server or other device.

Attack surface
Any device, system or person an attacker can use to gain access to sensitive data or make it unavailable. Organizations should consider their complete attack surface across all the devices, systems and employees when putting security defences in place. The attack surface has vulnerabilities (e.g., weaknesses) through which attackers launch threats (e.g., malware, phishing, privilege escalation).

Attacker
In this paper attacker and hacker are used synonymously and refer to an individual or organization either from outside a business or potentially inside that attempt to access data without permission or disrupt a business by making data or systems unavailable for normal use.

Authentication
A password, username or other login information entered or provided as proof that the particular individual is allowed to gain access to a smartphone, PC, cloud service, other system or device. Increasingly a fingerprint scan or other physical verification methods are being used in addition to traditional usernames and passwords.

Bootable copy
A complete backup or copy of the operating system, apps and data needed to run a device for everyday use. If a smartphone, PC or server gets attacked and has its data corrupted, then having a clean bootable copy available will help to quickly restore it to a working state.

Breach
Occurs when an attacker has gained access to a network, smartphone, PC, cloud service or any other device or system. It does not mean that sensitive data has necessarily been viewed, corrupted or made unavailable by the attacker. Rather, it is simply that a breach provides the ability to cause harm because entry into a system has been made.

Canadian Anti-Spam Legislation (CASL)
Canadian federal legislation that came into effect on July 1, 2014. CASL requires organizations to actively seek customer or prospect consent prior to sending them email, text or other electronic marketing communications. A business can be fined up to $10 million for noncompliance with CASL. The three-year grace period which began in 2014 expires on July 1, 2017, when all organizations must comply.

Certified information systems security professional (CISSP)
A recognized de facto standard in security training that indicates an individual has a minimum of five years of paid full-time experience in two or more of eight security domains, passed the CISSP examination, subscribed to the $(ISC)^2$ Code of Ethics and been endorsed by an $(ISC)^2$ certified professional. Recertification is required every three years and there are annual checks in place to ensure that security professionals stay current on new security developments.

Compliance
Indicates abidance to the standards, regulations or laws set out by industry associations, government agencies and/or international, federal, provincial or municipal governments. Professional auditors can be brought in to determine if proper security safeguards to meet compliance requirements have been established. Software can be installed to help ensure that security defences continue to achieve compliance.

Compromised
Similar in definition to a security breach but more serious. In this guide book we use compromise to mean that data has been viewed, copied, corrupted or made unavailable. The terms compromise and breach are often synonymous in security literature.

Corrupted
An attacker may change data in a way that makes it either partially or fully useless to an organization. For example, a ransomware attack fully changes every bit of data on a server, PC or other device and will be restored to its useful state by the attacker usually if money or ransom are paid.

Cybersecurity defences
See cybersecurity.

Cybersecurity
Practices, training and tools for the protection of electronic data. It should be part of an overall security strategy. Typically cybersecurity refers to protecting an organization from crime over the internet. It is derived from security of cyberspace.

Data loss prevention
This is a type of security software used to detect when important or sensitive data (e.g., financial, product specifications, customer data, other sensitive data) is being sent outside the organization when it shouldn't be. This may include data that shouldn't be sent outside a cloud service as well.

Distributed denial of service (DDoS)
This is a form of attack intended to reduce or completely deny users access to a Web site, online application, system or network. There are a number of ways an attacker can DDoS your organization, but primarily it involves sending more requests to the Web site or other network resource than it can handle. Think of refreshing a Web site on your Web browser, but doing that so many times a second that the site can't keep up. Defences include using solutions on the network that can filter out and reroute bad traffic, or allow your service provider to handle the attack by routing your traffic through their network (this is optimal for most organizations).

Defence-in-depth
Defence-in-depth means using multiple layers of security technology, monitoring and employee training to protect assets such as servers, PCs and smartphones. This means that there are multiple hurdles an attacker needs to traverse in order to gain access to sensitive data.

Drive-by attack/drive-by download
This occurs when an employee accidentally downloads a virus or other malware by clicking on what looks like a legitimate pop-up window in a browser. Attackers can also launch a drive-by download attack without the user taking any action. This is done by taking advantage of weaknesses (known as vulnerabilities) in (primarily older) browser technology.

Encryption
Data is converted into a form that is unreadable to anyone who doesn't have the keys to decode it. Most of today's smartphones come with data encryption built in. The keys are managed by software on the phone so the user does not need to actively encrypt and decrypt their data. Encryption is also carried out on the web with email and other services that use it to create a secure communications "tunnel" between a PC and the online service, for example. Most often users are unaware this extra security step is being conducted.

Endpoints
Any device connected to a network such as a smartphone, PC, server or IoT sensor.

Firewall
Like a literal firewall that stops a fire from spreading through a building, a security firewall is a barrier in a network that stands between less secure and more secure environments. It separates one part of a network from another to create safe zones for sensitive data/applications. Firewalls can take the form of software or a dedicated hardware appliance. Firewalls protect PCs and servers as well at connection points along a network.

IaaS
Infrastructure as a service is a cloud-based delivery model which provides customers with computing/server and storage resources. Similar to platform as a service but without platform capabilities such as development, runtime, database and other like services.

Incident response plan
A document that describes the necessary actions to be taken by staff in the event of a security breach. Such plans are particularly important to lay out what to do if personally identifiable information of employees or customers is known or suspected to have been exposed.

Intrusion detection and prevention (IDP).
Tools that flag unusual and potentially harmful activity on a network. Essentially, you or your provider put an IDP software or a hardware appliance on your network to watch for suspicious traffic — and block it.

Intrusion
Unauthorized access to your data achieved by hacking into your network, smartphone and other devices. In this guide breach and intrusion are synonymous.

IT security
Ensuring that physical devices and electronic data are protected from being viewed, corrupted or rendered unavailable by an attacker.

Keyloggers
This is a form of malware used by an attacker to capture keystrokes typed on a keyboard, including usernames and passwords. They can also capture a user's typing pattern which can be used to defeat some forms of authentication.

Malware
Any software that causes harm by attempting to gain access to or damage computing devices or systems. A virus is a form of malware. Software that defends a smartphone, server or other system or device is therefore called antimalware.

Managed security services provider (MSSP)
MSSPs are security services firms that have their own security operations centre (SOC) to watch for new threats 24 hours a day, 7 days a week in order to stay ahead of attackers. Organizations that subscribe to their services generally don't have the time, staff availability or in-house skills needed to monitor and manage the security of their network, PCs, smartphones, cloud services and other systems and devices.

Network segmentation
The separation of a network into zones or segments of higher and lower data sensitivity and application criticality. Think of an office with open WiFi for guests to use and the private network where only secured business data can be used. Larger organizations have many such segments for many layers of devices and levels of sensitivity.

Network
The physical and software-based connections between all devices and systems that make it possible to send data between them.

Next-gen endpoint
This is security software that organizations can purchase and download onto devices. It is a term created by security vendors to differentiate newer (e.g., machine-learning-based) approaches of securing PCs, servers and smartphones from traditional (also called signature-based) approaches.

PaaS
Platform as a service is a recurring fee-based service delivery model which allows customers to develop, test, run and manage their own applications through a cloud service. Similar to software as a service (SaaS) this cloud service does not provide applications. Instead, customers develop it on their own.

Passphrases
A password that is an easy-to-remember plain language phrase (e.g., a phrase such as the "Blue horse hopped a train to the clouds").

Password managers
Software that generates, stores and retrieves complex passwords from an encrypted database. The user only needs to remember one "master" username and password. This software reduces the need to remember or write down many passwords, increasing security by reducing the risk that passwords are reused or easily stolen.

Patches and updates
New features, improvements and functions are routinely added to most software and applications to ensure the latest attacker threats won't work against it by fixing vulnerabilities. Patches and updates apply new code to existing software to repair known vulnerabilities.

Payment Card Industry Data Security Standard (PCI DSS)
A regulation created by the payment card industry (e.g., credit card companies and banks) that carries fines for noncompliance. Any organization that collects payment via credit cards is subject to the fines. PCI DSS is regularly updated and the most recent 3.2 version was released in the spring of 2016. It has a list of security requirements that must be met by any organization that accepts credit card payments. The regulation is intended to ensure credit card data is kept safe by separating it from other customer data.

Penetration testing (also called pen testing)
The process carried out either by internal security professionals or an external security service provider intended to find vulnerabilities (weaknesses) in an organization's network, servers, web applications and/or other devices. The pen testers act as though they are an outside attacker trying to break in and utilize a variety of attacks to uncover weaknesses.

Personal Information Protection and Electronic Documents Act (PIPEDA)
Canadian federal legislation passed in 2004 designed to encourage organizations to safeguard consumer privacy. PIPEDA outlines how businesses need to transfer, store and secure personally identifiable information.

Personally identifiable information (PII)
Organizations in Canada must safeguard the personally identifiable information of customers and employees through processes and practices set out by federal and provincial laws. Included are many pieces of information such as date of birth, health information, salary, employee reviews, customer purchase history and anything else that if exposed could cause harm (e.g., reputation, financial, privacy).

Phishing
A type of attack, usually carried out over email, where an attacker tries to trick an employee or customer into revealing sensitive information (e.g., login information, banking details, company secrets) or taking an action (e.g., transferring money, sending a message to another party, launching a malicious piece of software). The attackers are "phishing" for someone willing to be hooked by their bait. Phishing may be carried out with a broad spam message sent to many people or it may be targeted at someone specific.

Physical security
Ensuring that any physical server, PC, smartphone or other system or device is protected from theft or damage. This can include placing a server behind a locked door, tethering a PC to a desk or making sure a smartphone is not left out unattended.

Privacy
A person's right to control their personal information and keep it confidential. It is not the same as security. Privacy is, in part, protected by using security technologies and training. In Canada, all organizations have a legal obligation to protect the privacy of employees' and customers' personally identifiable information.

Ransomware
This is a common variety of malicious software that infects PCs, servers, smartphones and other systems and devices. Users unintentionally install it on a system or device by clicking on a link in what they think is a trusted email or website, opening an infected attachment from email or the web, or downloading an infected application. Ransomware works by using encryption against a person to deny access to data. The attacker locks up important files and asks for a ransom to be paid in order to restore access. Often, the attacker demands to be paid electronically in bitcoin so the transaction can't be easily traced.

Remote wipe
A service or software that allows an administrator or device owner to send a command that erases the data on a device such as a computer or phone.

Risk/risk plan
(see security risk plan).

SaaS
Software as a service is a recurring fee-based service delivery model in which applications are provided on a subscription basis (paid monthly or annually) from a central location. Subscribers access the application via the internet. SaaS is the most common form of cloud computing including email, sales, accounting and other services offered over the internet.

Secure Sockets Layer (SSL)
This is a standardized implementation of encryption technology most commonly used for securing the connection between a device and a web-based service such as email and banking web sites.

Security appliance
A firewall or any other security functionality that an organization purchases as a piece of hardware. It is the same as buying software, but the software comes built into the appliance with all the network, server and storage capabilities optimized for ease of use.

Security information event management (SIEM)
Tools to watch activity across devices on the network to provide early warning signs of an attack by correlating events from multiple sources. Midmarket or larger Canadian organizations with bigger networks and dozens if not hundreds or even thousands of servers use these solutions.

Security maturity
This is an assessment of the level of sophistication with respect to security or cybersecurity. Organizations should try to progress to higher levels over time. Progress is considered within several areas such as technology, training, and security risk and incidence response planning.

Security policy
A documented set of rules, guidelines and actions that an organization uses to improve its security safeguards. Information security policy and acceptable use policy are two common security policies. For example, a policy can describe which employees (administrator, manager, director, etc.) have access to which company data.

Security posture/cybersecurity posture
Refers to all technologies, processes, planning and training an organization has stood up or otherwise put in place to defend against an attack.

Security risk plan
A document in which an organization spells out how it will weigh the costs of preventing an attack from happening versus the damage that might occur if nothing/something less is done. An organization begins by taking an inventory of assets, assigning a value to the assets, determining the likelihood something bad might happen, calculating the potential loss, prioritizing the appropriate defences, deploying the defences and measuring the effectiveness of the defences once deployed.

Server
A storage and processing computing device accessed by multiple people simultaneously.

Social engineering
Any attack that convinces an employee or other stakeholder to provide sensitive information to a party that wasn't supposed to see it. This can take many forms, from impersonating a business partner over the phone to gaining entry into an office by faking a delivery to using social media to masquerade as an executive of a company.

Spam
Unwanted electronic messages sent in large quantity to a multitude of email addresses, voice mail inboxes and text numbers.

The Digital Privacy Act
Canadian federal legislation passed in 2015 to add, update and strengthen several sections of PIPEDA (see PIPEDA definition) including mandatory breach notification. This legislation, in certain circumstances, directs companies to inform the government and customers when a privacy breach occurs. It established stiff penalties for organizations that don't comply.

Threat intelligence
A service that determines where and how new threats are forming. This is often a feature of managed services and increasingly a built-in function of some firewalls and other network defence technologies.

Threat
Defines different ways that an attacker might view, corrupt or otherwise make business data or systems unavailable. How the attacker may cause harm to a business is a threat. Ransomware, phishing and physical theft of devices are examples of threats an attacker may use to cause harm.

Trojans
This is a form of malware an attacker uses to disguise malicious software within something trusted such as a document file or an application. The Trojan file or application is released when it is downloaded or activated on a PC, smartphone or other system and may act as a gate for other attacks.

Two-factor authentication
Requiring a user to provide two things in order to gain access to a system or device. This is done to make it more difficult for an attacker to break in. In security circles it is described as any two of "something one has, something one is and something one knows." Entering a password and scanning a finger is a typical example of two things one does to access a smartphone. Inserting a bank card into an ATM followed by entering a PIN is another example of two-factor authentication. See also authentication.

Virtual private network (VPN)
This security solution extends a secure private network over the public internet making it seem like the device is directly connected to the private network. A secure encrypted "tunnel" is created to ensure attackers can't view data as it travels across the network. See also Secure Socket Layer (SSL), which is a type of VPN.

Vulnerability scanning
A technique to look for any network or software flaws/weaknesses that an attacker could use to cause harm to your data or systems. The next step after a vulnerability scan is to fix the problems that have been identified.

Vulnerability
A weakness in a device or system that attackers can exploit to their benefit. Vulnerabilities take many forms, including software that hasn't been updated, an employee's lack of security knowledge, a misconfigured firewall, an unlocked PC and an open/unsecured WiFi connection. A vulnerability is different from a threat in that a vulnerability is the weak point or link from which a threat can be launched.