

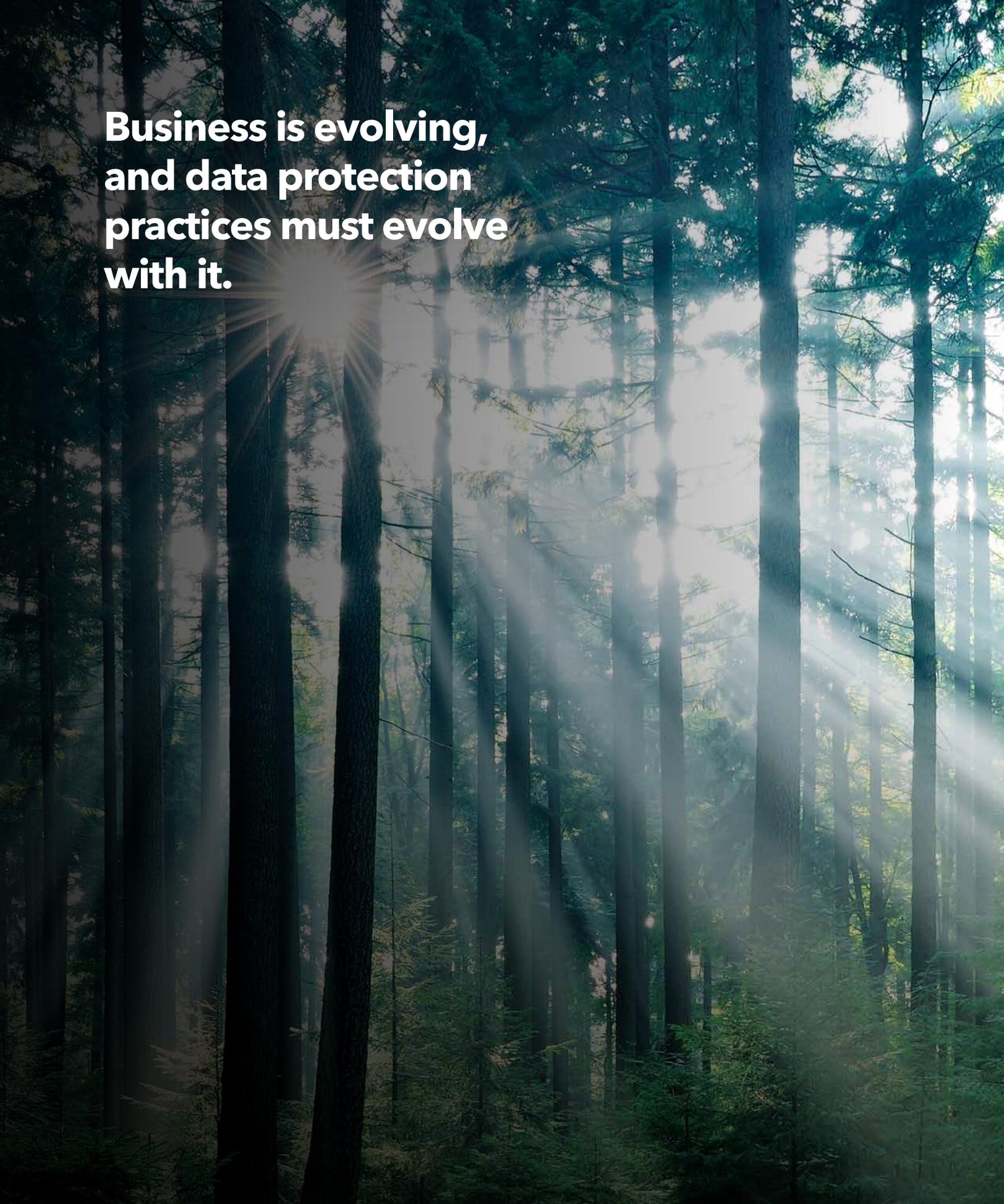


# State of the Industry

Information Security

2018 NORTH AMERICA





**Business is evolving,  
and data protection  
practices must evolve  
with it.**



Introduction	3
Situation Analysis: Canada	4
Situation Analysis: United States	7
Security Tracker Infographic	8
The Evolving Workplace	10
Physical Safeguards: People and Places	12
Data Privacy: Adopting a Global Mind-Set	13
Addressing Growing Consumer Concerns	14
Ask the Expert	16
Legislative and Consumer Sentiment Trends	18
Summary	20

A high-angle, close-up photograph of a person's hands typing on a silver laptop keyboard. The laptop is open on a dark wooden table. To the left, a hand holds a tablet displaying a document. In the foreground, a hand is writing in a spiral notebook. A smartphone lies on the table next to the laptop. In the background, another person's hands are visible, one holding a smartphone. There are two clear glasses on the table. The overall scene suggests a collaborative work environment.

**After a turbulent year marked by growing concerns about privacy, business leaders need to reassess how they protect their organizations from potential security risks and breaches.**

# Introduction

Every year, Shred-it's State of the Industry Report aims to help businesses understand the risks they face in a world dominated by technology. The report draws on the detailed findings from the annual Shred-it Security Tracker, an in-depth targeted research study conducted on behalf of Shred-it by Ipsos. Now in its eighth year, the 2018 Security Tracker study provides global insight on information security policies and procedures among Small Business Owners (SBOs) and C-Suite Executives (C-Suites) in the United States, Canada, the United Kingdom and Australia.

This international outlook gives readers insight on emerging risks and highlights how businesses in different countries prioritize data protection and information security. The 2018 State of the Industry Report reveals a number of common themes and emerging challenges, including:

## Legislative Changes:

Europe's General Data Protection Regulation (GDPR) came into effect as of May 25, 2018, affecting businesses all over the world. This, combined with growing talks of stricter privacy legislation in the United States and Canada, means North American businesses will need to do more to adhere to data protection standards.

## Evolving Work Styles:

As working from home and open-concept offices become increasingly popular, businesses are put at greater risk of data breaches caused by human error. To mitigate this risk, they will have to adapt their security measures and keep up with changing workplace standards.

## Employee Training:

The majority of North American businesses are confident in their employees' efforts to safeguard company data, yet most do not provide staff with regular training on information security procedures. Ironically, many businesses still place responsibility for data security on their employees.

## Customer Concern:

The number of data breaches experienced by North American businesses has grown since last year. According to the Shred-it Security Tracker, C-Suites in the U.S. reported a 10-point (22 percent to 32 percent) jump in breaches since 2017, while Canada had a 6-point (18 percent to 24 percent) increase. As a result, customers are becoming more concerned—and more savvy. Our research shows North American consumers place high importance on data protection when deciding which bank to use, where to buy a car, which hotels to stay in and even where to work.

Falling victim to a data breach can be devastating to a business of any size. Financial loss, reputational damage, and loss of customer trust are only some of the long-lasting effects of a breach.

To learn how you can protect your company, people and customers from fraud, visit the Shred-it Resource Center at: [Shredit.com/resource-center](https://shredit.com/resource-center).

## Situation Analysis: Canada

Insufficient employee training and inadequate security policies have left Canadian businesses at risk for data breaches.

Businesses across Canada are making themselves vulnerable to breaches, leaving customer data exposed and risking their reputations. Our research shows that Canadian businesses are not addressing known and perceived security risks with the proper training, policies and/or enforcement mechanisms. This is worrisome, considering many businesses report adopting working styles such as open concept offices and remote work, both of which increase the risk of breaches.

As of this year, 89 percent of large businesses and 50 percent of small businesses use flexible and/or off-site work models. The majority of C-Suites (82 percent) and SBOs (63 percent) feel the risk of a data breach is higher when employees work off-site. Despite this, only 64 percent of C-Suites and 43 percent of SBOs are confident that their employees understand their data storing and disposal policies.

Small businesses need to do more to protect customer data. Only 56 percent have a policy for storing and disposing of confidential data on paper documents, compared to 92 percent of large organizations. In addition, only 45 percent of SBOs report having a policy in place for end-of-life electronics and 56 percent do not have policies for storing and disposing of confidential information when working off-site. Small businesses in Canada have a lot of work to do if they want to catch up with information security best practices.

Larger companies are more proactive when it comes to developing and enforcing corporate policies on information security, but they too face challenges. Though the vast majority have policies related to data protection, 28 percent say that not all employees are aware of such policies. Additionally, only 59 percent of C-Suites report training staff on information security procedures at least once a year. However, having policies in place is not enough. Large Canadian companies need to implement better training practices to protect their data and their reputations.

External factors like customer concerns and stricter legislation should motivate Canadian businesses to improve their information security standards.

Among the general population, a large majority of Canadians see data protection as an important factor when making big decisions—with the majority saying data protection is important when deciding which bank to use (85 percent), considering where to work (79 percent) and determining which legal firm to hire (77 percent). Moreover, 94 percent of Canadians see employee negligence as at least a minor contributor to data breaches—with 31 percent seeing it as a major contributor.

In addition to heightening internal security standards, Canadian businesses also need to comply with new regulations like Europe's General Data Protection Regulation (GDPR), in effect as of May 25, 2018, and amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA), which will come into effect November 1, 2018. These regulations are timely, given increasing concern about how companies are handling consumer data. Cambridge Analytica's misuse of Facebook data is a prime example of what is driving this sentiment.

With new rules in place and much talk in the last year about security concerns, it is in the best interest of both small businesses and larger companies to boost their information security measures. By putting better policies in place, providing regular employee training and adapting security measures to changing work styles, Canadian companies have the opportunity to minimize risks to their business and regain customers' confidence.



**Canadian businesses are not addressing known and perceived security risks with the proper training, policies or enforcement mechanisms.**

A man in a dark suit and tie is sitting at a desk, looking at a laptop. He has his hand on his chin, appearing thoughtful. A smartphone is on the desk next to the laptop. The background is a blurred office setting with warm lighting.

**96%**

**of Americans think  
employee negligence  
contributes to breaches.**

## Situation Analysis: United States

On the path to total information security, the biggest obstacle U.S. companies face is their own staff.

The vast majority of C-Suites (84 percent) and half of SBOs (51 percent) in the United States identify employee negligence as their biggest information security risk. Likewise, almost all American consumers (96 percent) view employee negligence as a contributor to data breaches at U.S. companies.

Most American business leaders—86 percent of C-Suites and 60 percent of SBOs—also believe the risk of a data breach is higher when employees work remotely. With 88 percent of C-Suites and 48 percent of SBOs using flexible and/or off-site working models, U.S. business leaders need to keep pace with modern workplace trends and adapt their security measures accordingly.

Our research shows that businesses are right to be concerned. Out of the 32 percent of C-Suites and 3 percent of SBOs that report experiencing data breaches in the past year, 69 percent of breaches reported by C-Suites and 71 percent of breaches reported by SBOs are at least in part attributed to employees—whether through human error or accidental loss (47 percent C-Suites, 42 percent SBOs) or deliberate theft or sabotage (22 percent C-Suites, 29 percent SBOs).

Despite the potential and actual risk posed by employee negligence, most U.S. businesses do not offer adequate data security training to their staff. Though 89 percent of C-Suites have a policy for storing and disposing of confidential data on end-of-life electronic devices, for example, 18 percent say that not all employees are aware of such policies. Since only 78 percent report training their staff on information security procedures and policies at least once a year, the reason for this discrepancy is clear. Small businesses face a bigger challenge, as only 34 percent even have such policies in place.

Overall, both C-Suites (99 percent) and SBOs (82 percent) report having an understanding of the legal requirements for handling confidential information in their industry. To properly protect their businesses, however, they will have to ensure that employees are properly trained and updated on the latest regulations.

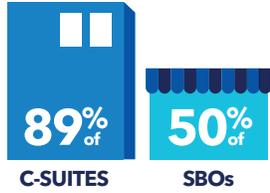
**Keeping up with and training employees to follow new legislation should be a priority for U.S. companies.**

With the European General Data Protection Regulation (GDPR) in effect as of May 25, 2018, U.S. companies doing business with European Union residents now have even more legislation dictating the way they gather, store and handle data.

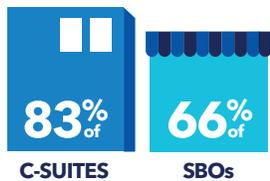
Furthermore, Cambridge Analytica's mishandling of Facebook users' data has also sparked discussion and debate about the U.S. government's role in regulating the collection, usage and sharing of data by American companies. When Facebook CEO Mark Zuckerberg testified before the Senate and House committees in April 2018, legislators made it clear that the government may need to step in if companies do not take adequate precautions to prevent breaches or misuse of customer data.

## CANADIAN BUSINESSES THAT...

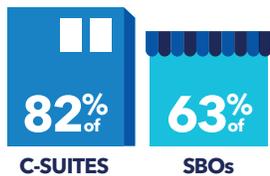
Have employees who work remotely:



Believe remote work will become even more important in the next five years:



Agree the risk of a data breach is higher when employees work remotely:

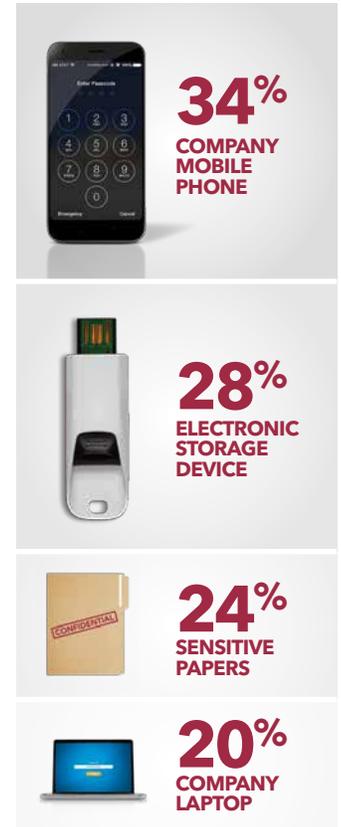


# REMOTE WORK EXPOSES BUSINESSES TO RISK

Canadian employers must take steps to protect against breaches when employees take sensitive data off-site.



Sensitive items lost or stolen while C-Suite business employees were working off-site:



## ALL SECTORS MUST PRIORITIZE DATA PROTECTION

Canadian consumers say data protection is important when choosing:

Which bank to use

**85%**



Their place of employment

**79%**



Which legal firm to hire

**77%**



At which hotel to stay

**74%**

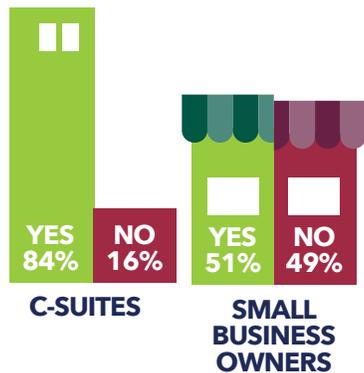


From which dealer to buy a car

**72%**



Is employee negligence one of the biggest information security risks?

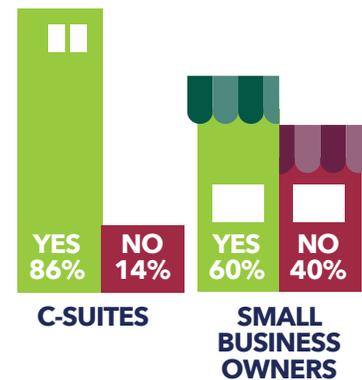


## EMPLOYEE NEGLIGENCE IS A TOP DATA BREACH CONCERN IN THE U.S.

U.S. businesses must make employee training a top priority to protect sensitive data.



Is the risk of a data breach higher when employees work remotely?



### CONSUMERS AGREE:



**96%** of Americans see employee negligence as a contributor to data breaches.

### HALF OF C-SUITES



say human error or accidental loss by an insider caused a data breach.

## ALL SECTORS MUST PRIORITIZE DATA PROTECTION

American consumers say data protection is important when choosing:

Which bank to use

**92%**



Which legal firm to hire

**83%**



Their place of employment

**81%**



At which hotel to stay

**77%**



A car dealership

**75%**



# The Evolving Workplace

As companies continue to evolve the way they do business, working styles are also changing and adapting to industry trends. Working remotely or in an open-concept office can benefit both employers and staff, but business leaders should adapt information security protocols to mitigate any additional risks from these work environments.

## Remote Work

Working remotely has increased in popularity over the last few years—and it has never been easier. Whether employees consider their living room a permanent office or need to spend a few days at home to take care of a sick child, increased connectivity and technological advancements make it possible to work from almost anywhere. As of 2017, most C-Suites in the United States (88 percent) and Canada (89 percent) and a large proportion of small U.S. (48 percent) and Canadian (50 percent) businesses reported using flexible or off-site working models.

Offering a flexible working model benefits employers, allowing them to attract top talent without geographical or time constraints. Working remotely can also increase productivity, letting employees focus on important work without being interrupted by colleagues or being distracted by general office mayhem. Most C-Suites in the U.S. (88 percent) and Canada (83 percent) believe that the option to work remotely will become increasingly important to their employees over the next five years, as do roughly 65 percent of North American SBOs.

In their eagerness to implement this model and benefit from employees working off-site, many employers have failed to adjust their data protection policies for exposure to new potential risks. Over 90 percent of North American C-Suites say they trust their employees are doing everything they can to safeguard sensitive information when working off-site, but 49 percent of C-Suites in the U.S. and 20 percent of C-Suites in Canada report that company laptops have been lost or stolen, while around 43 percent of C-Suites in the U.S. and 34 percent of C-Suites in Canada report that company mobile phones have been lost or stolen.

The majority of C-Suites in the U.S. (80 percent) and Canada (74 percent) do have policies for storing and

disposing of sensitive data for employees working off-site, but 13 percent and 16 percent, respectively, confess that not all employees are aware of these policies. Small businesses fare worse, with 54 percent of U.S. and 46 percent of Canadian SBOs saying they do not have a policy in place at all. The issue may be further confused if employees do not understand what constitutes sensitive data. Information security policies should clearly define what is considered sensitive data, and businesses should ensure this is emphasized during regular training.

Employees working remotely can expose businesses to both physical and digital breaches, so it is important to have policies and safeguards in place. Businesses need to address these added security risks with proper training, policies and enforcement mechanisms. With 94 percent of C-Suites in the U.S. and 79 percent in Canada saying they audit their security procedures and policies at least once a year, these audits could be a good opportunity for business leaders to take extra precautions with off-site workers.

## Open-Concept Offices

Often sleek, modern and technologically advanced, open-concept offices have become increasingly popular in the last few years. This set-up is said to increase collaboration, but it also increases the risk of data breaches. Fewer doors mean fewer locks and therefore fewer opportunities for safeguarding sensitive documents, both electronic and physical.

In open-concept workplaces, sensitive information is often on display with nothing stopping prying eyes from peeking at confidential data. When modernizing their working environments, employers should take precautions to mitigate the increased risks of open offices. The best way to do this is to have solid policies in place and provide thorough and regular training to employees.

In addition to policies on storing and disposing of confidential data and end-of-life electronic devices, employers can encourage employees to take security into their own hands. A Clean Desk policy, for example, would require employees to keep sensitive or confidential information out of sight, for example in a locked drawer or cabinet.

A woman with long brown hair, wearing glasses and a white and blue striped sweater, is sitting on a chair. She is looking at a smartphone in her right hand. In front of her is a silver laptop with a blue screen. To her left is a red handbag with gold jewelry. The background shows a wooden chair and a table. The text is overlaid on the right side of the image.

**Over 80%**  
of North American C-Suites  
believe the risk of a data  
breach is higher when  
employees work off-site.

## Physical Safeguards: People and Places

With so much information now stored digitally, it is easy to think that strong IT defenses are enough to keep your data protected. There are other ways to gain access to confidential data, however, and they do not involve a hacker behind a computer screen. Physical data protection measures should be top-of-mind for businesses collecting and handling sensitive information. This includes having a good alarm system and security cameras, keeping file cabinets locked, properly disposing of sensitive documents and old hard drives, and having a policy for mobile devices.

Training is also critical to safeguarding your sensitive information. If employees are not properly trained to mitigate risks, businesses could be exposing themselves to potential breaches. Most C-Suites in North America (96 percent in the U.S. and 91 percent in Canada) provide

some form of training on physical information security to their employees, but only 45 percent of SBOs in the U.S. and 52 percent in Canada report doing the same.

Our research found that businesses across the continent are most likely to train employees to keep sensitive information out of sight when working in a public space, report a lost or stolen electronic device and identify fraudulent emails. Existing training policies did have some gaps, with fewer businesses cautioning employees against sharing electronic devices with family and friends, using public Wi-Fi and keeping company-issued devices safe from interference at home.

### Implement these physical safeguards to protect your data:

#### ✓ Secure physical access to information

Inside the office, make sure you store confidential information in locked cabinets, storage rooms or in password-protected files. Implementing a Clean Desk policy, which requires all employees securely store documents and devices when they are not at their desks, is a great way to ensure sensitive information stays out-of-sight. Encourage employees to keep sensitive data in digital form only. If it is necessary to keep hard copies, ensure they are destroyed properly when they are no longer needed.

#### ✓ Evaluate third-party access to confidential information

Many third parties require confidential information to provide services. In 2018, 72 percent of U.S. and 91 percent of Canadian C-Suites who reported suffering a breach attributed it, at least in part, to an external vendor or source. Audit the security and privacy policies of your third-party vendors and ensure they have clearly established contractual obligations to notify you in the event of a data breach.

#### ✓ Develop a corporate mobile device policy

With flexible work models and variable hours becoming the norm, employees are more likely than ever to have confidential information stored on their mobile devices. Once those devices leave the workplace, employers often lose track of what happens to them. Create a Mobile Device policy that helps control the use of these devices.

#### ✓ Properly dispose of old hard drives

Confidential information remains on a hard drive even if the data has been erased, deleted or reformatted. Thieves can use specialty software to recover data even if the original user deleted it from a device. Hard drives and other electronic materials containing confidential information should be securely wiped or destroyed.

# Data Privacy: Adopting a Global Mind-Set

In today's global and digital economy, companies of all sizes are collecting and handling sensitive consumer information from all over the globe. Businesses in the United States and Canada need to be mindful of not only local but also international regulations governing access to and usage of personal data.

The General Data Protection Regulation (GDPR), for example, came into effect on May 25, 2018, and will have repercussions for any business handling data on individuals located anywhere in the EU. Despite the importance of complying with this new legislation, only 22 percent of C-Suites in the U.S. and 13 percent in Canada report a strong familiarity with GDPR, and roughly 3 percent of SBOs across North America can say the same. A shocking 51 percent of American SBOs report not knowing anything about GDPR.

Adopting a global mind-set means not only adhering to the rules and regulations set by other countries when dealing with their residents, but also taking a holistic approach to data security and privacy. By incorporating information security into all aspects of their operations, business leaders can help create a global environment in which data risks are minimized and consumers trust companies with the information they need to deliver products and services.

## If you find yourself in the majority of business leaders who need to brush up on GDPR, here is a summary:

### What is GDPR?

GDPR is a legally-binding set of guidelines for collecting and processing the personal information of EU residents. While governing the way that data is handled, GDPR also gives individuals greater control over their own information.

### Who does it affect?

GDPR affects any company, individual or organization that collects or handles the personal data of the residents of any EU member country.

### What is personal data?

Under GDPR, personal data is defined as anything that allows for the identification of a living person, directly or indirectly. Some examples include names, phone numbers and both physical and IP addresses.

### What does this mean for my business?

GDPR demands data protection by design and by default. In short, data protection should be fundamental to your operations and should be incorporated into all business processes for the products or services you provide. Ideally,

you would collect as little data as possible and keep it separate from information about customers from non-EU countries to minimize risk.

A big part of GDPR is giving consumers easier access to data collected about them and erasing their data if the consumer requests this, which they may do in a number of situations—including if it is in the interest of their fundamental rights and freedoms. To comply with this, you need to ensure that you have a comprehensive data management system in place that can identify and carefully document that data.

GDPR also outlines a strict procedure in the event of a data breach. If you experience a breach, you are under legal obligation to disclose it within 72 hours unless the breach is unlikely to pose a risk to the individuals' rights and freedoms. Fines for failing to comply can reach up to US\$24 million (€20 million).

# Addressing Growing Consumer Concerns

North American consumers are increasingly concerned about the security and privacy of their data. In 2018, 32 percent of C-Suites in the U.S. and 24 percent in Canada report that their organizations experienced data breaches. Out of those who experienced breaches, one of the biggest consequences reported is harm to the organization’s credibility and reputation. It can take a long time for businesses to recover from data breaches. With fewer staff and resources, small businesses usually take a harder hit: over 60 percent of SBOs in North America say it took their businesses more than six months to recover, while some say they never fully recovered.

Consumers are getting savvier and more informed about data security issues following a number of high-profile breaches and instances of improper data handling—like the Facebook and Cambridge Analytica incident. Americans and Canadians have started demanding better protection and more information about how their data is being stored, distributed and used. To prevent long-term financial and reputational harm, businesses should listen to these concerns and take steps to address them.

Some sectors may have more work to do than others. Our research found that customers place a high importance on data protection when dealing with banks, law firms, hotels and car dealerships.

## Consumers say data protection is important when making big decisions like:



Internally, businesses should take all appropriate precautions with consumer data. This includes having comprehensive policies in place to protect data and address breaches if they occur, and regularly training employees on how to follow those policies. Externally, organizations should ensure that users or customers are told and understand both how their data is being used and what safeguards the organization has in place to protect that information.

Part of protecting consumers can also mean educating them about how to minimize risks to their own information.

By addressing consumers' concerns about the way businesses handle sensitive information and communicating the shared responsibility of consumers to safeguard their data, organizations across North America can also protect themselves from the financial and reputational consequences of breaches.

## The average person can help safeguard their data in a few simple ways:

- 1 Using strong passwords for all electronic devices and online accounts
- 2 Locking phones and computers when they are not being used
- 3 Never leaving laptops or mobile devices unattended in public spaces
- 4 Always logging out of websites and accounts on shared or public computers
- 5 Safely disposing of end-of-life electronics and data storage devices like USB drives



# Ask the Expert

## Imran Ahmad

Imran is a Business Law partner at Miller Thomson LLP, a leading Canadian law firm, and specializes in the areas of cybersecurity, technology and privacy law.

As leader of the cybersecurity and data breach practice, Imran works closely with clients to develop and implement practical and informed strategies related to cyber threats and data breaches. He focuses on legal risk assessments, compliance, due diligence and risk allocation advice, security and data breach incident preparedness and response. He also provides representation in the event of an investigation, an enforcement action, or a litigation.

Imran is a board member of the Canadian Advanced Technology Alliance's (CATA) Cyber Council which advises the Government of Canada on cybersecurity matters. He is an adjunct Professor at the University of Toronto where he teaches Cybersecurity and Privacy Law. He is also the Chair of the Executive Committee of the Ontario Bar Association's Privacy and Access to Information Law Section, and author of Canada's first legal incident preparation and response handbook titled A Handbook to Cyber Law in Canada.

### **How does the introduction of GDPR in Europe affect businesses in North America?**

**IA:** The General Data Protection Regulation ("GDPR"), which came into force on May 25, 2018, is a game changer when it comes to privacy and data protection, both within the European Union ("EU") and globally. It has extra-territorial scope, meaning that an organization that has no physical location in the EU but that collects, uses or discloses personal data of EU domiciled individuals may be caught and will need to comply.

The GDPR prescribes minimum privacy, data protection and information governance requirements that must be met by organizations when handling personal data of EU domiciled individuals. These range from maintaining records and registers of data processing by any third party, the right to be forgotten, data breach notification, the manner in which to obtain consent, etc. These requirements are often more prescriptive than current American and Canadian requirements.

Lastly, the cost of non-compliance can be significant. Violations of the GDPR could result in administrative fines of up to 4 percent of annual global turnover or €20 million, whichever is greater.

### **What is the biggest challenge businesses face when it comes to information security and what steps can they take to mitigate the risk?**

**IA:** While there are many potential risks facing businesses when it comes to information security, the most important one remains the "insider threat". There are several surveys that confirm that no matter how much an organization spends on technology, the single most important point of vulnerability in an organization remains its employees.

The threat can come from two main sources. The first are employees that are not sufficiently trained on the business' security practices or who do not pay attention to internal security protocols and policies. This often results in employees making poor decisions or mistakes that result in a security breach. The second are "malicious" employees who are intentionally taking steps to harm the organization. They may be disgruntled employees who received a negative performance review, for example.

To address this threat, businesses should invest in frequent security staff training which should include physical and cybersecurity components. Emphasis should be placed on staff being able to flag issues and dealing with them effectively. Businesses should also implement internal monitoring protocols to quickly identify and respond to the "malicious" employee threat. This can include working with human resources and implementing technological monitoring solutions.

### **What are the common attributes of businesses that are highly successful in dealing with information security?**

**IA:** Businesses that successfully deal with information security are those where everyone, starting from the Board of Directors (the "Board") all the way down to the frontline employees are directly engaged and know that they have an important role to play.

The Board and Senior Leadership Team should be responsible for setting the foundation around information security. By mandating the Operational Team within the business to develop, implement and monitor an information security program, they will be sending a strong message that information security needs to be taken seriously.

The Operational Team will also play an important role by virtue of being the conduit through which the information security plan will be implemented throughout the business and issues that arise will be relayed back to the Board and Senior Leadership Team for action. This can include, for example, recommendations by the Operational Team to the Senior Leadership Team that additional resources (e.g., technology upgrade, hiring of security staff, etc.) may be required to meet minimum security requirements.

This constant loop going up and down between the Board, the Senior Leadership Team, the Operational Team and frontline employees is the single most important element to a successful information security framework.

**Workplaces are evolving with a trend toward flexible and remote working arrangements. What data security risks do these types of work arrangements present and what can employers do to protect sensitive data?**

**IA:** Flexible and remote working arrangements are here to stay and businesses need to embrace it or risk losing talented employees. However, there are inherent risks to these types of arrangements. For example, failure to use company mandated technology and hardware may result in employees using their own devices or computer programs that are not secure, potentially resulting in information security breaches.

To avoid issues, employers should consider what type of access each employee should have when working remotely. For example, there are ways to limit an employee's access to only the data that is necessary to their day-to-day tasks, thereby precluding them from accessing the organization's entire universe of data. Another example is blocking or prohibiting the use of public Wi-Fi, which can represent a significant risk from an information security standpoint.

Some common best practices include offering employees company issued laptops (or other devices) which are closely managed and monitored by its security professionals. Another step would be to encrypt data transmissions. An additional security step can include remote "wiping" of data in the event a given hardware is lost or installing additional security layers so that an unauthorized user cannot access the data on the device.

**What impact did the recent privacy scandal involving Facebook and Cambridge Analytica have on how governments and businesses approach data security?**

**IA:** The Facebook/Cambridge Analytica incident was significant not only because of the actual unauthorized use of personal data, but also because it highlighted that organizations collecting large amounts of data need to be careful when they transfer this data to third-party service providers.

As a general rule, a business will typically rely on a third-party service provider for different aspects of data and information management. This ranges from cloud storage to conducting data analytics to glean helpful insights. However, as the entity that is collecting the data in the first instance, the business has a legal responsibility to carefully vet any third-party service provider that it may be relying on and to monitor their operations to ensure their compliance with applicable laws and any contractual terms to which the parties agreed.

Accordingly, having robust contractual language with third-party service providers on how the data can be used and ultimately returned or destroyed to the business is extremely important. In addition, however, the business should have means to verify compliance by the third-party service provider. This can include compliance audits or even on-site visits. Either way, businesses transferring data should follow the saying: "Trust but Verify".

## Trends in Legislation and Consumer Sentiment

Since news broke that Cambridge Analytica misused Facebook users' data, many print and online publications have started pushing readers to protect their own data in any way they can—but users can only do so much. The internet's rapid takeover of commerce and communications erased national borders years ago, so it makes sense for data protection laws to evolve accordingly.

### GDPR

Leading this evolution is the European General Data Protection Regulation (GDPR). As one of the most significant changes in European data legislation in over 20 years, GDPR came into full effect on May 25, 2018, after a two-year transition period. These new rules aim to protect the data of European Union residents and give them greater control over their personal information. Though GDPR is considered a European law, any country accessing the data of EU citizens must adhere to it.

GDPR already seems to be setting data protection standards beyond European borders. Current and upcoming regulations in Canada and the United States are fairly light compared to GDPR, and many see them as inadequate and feel that stricter laws should be in place. In a move to appease concerns over Facebook's access to personal data, CEO Mark Zuckerberg has said that the company would make the same controls and settings implemented under GDPR available globally.

### Canada: PIPEDA

Canada's federal government has been considering data breach regulation measures for the past three years. In April 2018, the Minister of Innovation, Science and Economic Development announced amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA) that will address some concerns related to data breaches by Canadian businesses.

As of November 1, 2018, organizations across Canada subject to PIPEDA will be required to provide notice of certain privacy breaches. Under the new regulations, businesses will need to assess whether a breach presents a real or significant harm to individuals and, if it does, disclose said breach to both the individuals affected and to the Office of the Privacy Commissioner.

In the past two years alone, large Canadian companies like Bell Canada, Loblaws and Canadian Tire experienced significant breaches to consumer data. Issues arise when some of these businesses take too long to notify consumers of data breaches—as was the case for Canadian Tire—or when they only notify them after being prompted by legislative action.

The government seems to hope that amendments to PIPEDA will address some of the concerns that arose from the events mentioned above. In fact, our research shows



that Canadian C-Suites have an overall positive (73 percent) impression of the government's response and commitment to information security, with 52 percent of SBOs agreeing. It seems many Canadian business leaders would like the government to do more. With growing concerns over data security and GDPR setting an example on the global stage, Canada may soon grant that wish.

### United States: Getting Serious About Privacy

In the past two years alone, large U.S.-based companies like Facebook, Uber and Yahoo experienced breaches or misuse of data that affected customers world-wide. Not only did these breaches affect each company's reputation, they sparked bigger concerns and conversations about data security and privacy. With little done to protect consumers during such events, many are looking for the U.S. government to step in. Though 61 percent of American C-Suites give their government an overall positive grade for their response and commitment to information security, 58 percent of SBOs say it needs improvement and 13 percent of SBOs say it is abysmal.

In the aftermath of Cambridge Analytica's misuse of Facebook data, the United States government is pushing for more regulation governing data protection and privacy. In April 2018, when Facebook CEO Mark Zuckerberg

testified before the Senate and House committees, many Senators and Representatives had a common message to everyone watching: if U.S. companies cannot be trusted to keep consumer data safe, the government will step in and regulate how that data is handled.

Consumers and government representatives are not the only ones expressing concern. In late April 2018, WhatsApp CEO and co-founder Jan Koum announced he would be leaving the company after ideological clashes with parent company Facebook. Though the announcement happened in the wake of the Cambridge Analytica scandal, Koum's departure came after he expressed concern over Facebook's attempts to weaken WhatsApp's encryption and use personal data from the app in order to monetize it.



## Summary

Shred-it is proud to provide businesses of all sizes with advice and data security intelligence based on our research. The 2018 State of the Industry Report highlights the main information security trends experienced by businesses and consumers across North America this year and outlines important actions those businesses need to take to protect themselves against data breaches.

Increasing threats to data security and the changing business landscape are pushing North American companies to do more to ensure the protection of consumer data. Whether that means investing in regular and thorough employee training, increasing physical safeguards or implementing stricter data policies, they have a responsibility to their customers and employees.

New legislation also means that businesses are increasingly accountable to their governments and other governments around the world. With GDPR already being enforced, PIPEDA coming into effect in Canada in November 2018 and talks of stricter legislation in the United States, North American businesses will need to keep up with and adhere to more and more regulations.

A good way for C-Suites and SBOs to uphold their duties to consumers and government alike is to integrate data protection into everything they do. Businesses should regularly assess their information security strategies and ensure they are keeping pace with changes in regulation and societal expectations.

For more tips on improving your information security, please visit the Shred-it Resource Center at [Shredit.com/resource-center](http://Shredit.com/resource-center).

 [facebook.com/shredit](https://facebook.com/shredit)

 [linkedin.com/company/shred-it](https://linkedin.com/company/shred-it)

 [@Shredit](https://twitter.com/Shredit)



**Data protection must  
become a core part of  
all business practices.**



# How Shred-it® Can Help

## The Shred-it Protected Workplace

Our integrated suite of products and services—including Paper Shredding, Hard Drive Destruction and Workplace Security Policies, all delivered through a secure Chain of Custody—are designed to protect the things that matter most, every single day.

## Shred-it Secure Document and Hard Drive Destruction

- » Secure end-to-end chain of custody processes
- » Certificate of Destruction after every service
- » Tailored solutions to your organization's needs

## Advice and Expertise

- » Trained experts in information security
- » Provide a Data Security Survey at your organization to identify information security risks

**Learn more about information security  
at [shredit.com](http://shredit.com) or 844-342-7499**

### 2018 Security Tracker Survey Methodology

Ipsos conducted a quantitative online survey of C-Suites and Small Business Owners (SBOs) in both Canada and the United States. We sampled a total of n=1,002 SBOs in Canada and n=1,003 SBOs in the U.S. and a total of n=100 and n=101 C-Suites in Canada and the U.S. respectively. Data for SBOs is weighted by region whereas C-Suites is unweighted as the population is unknown. The precision of Ipsos online surveys are calculated via a credibility interval. Both SBO samples are considered accurate within +/- 3.5 percentage points whereas C-Suites are accurate within +/- 11.2 and 11.1 percentage points in Canada and the U.S. respectively. The field-work was conducted between April 3rd and 18th, 2018. Ipsos also conducted a short omnibus survey among a gen pop sample of n=1,002 respondents in both countries about data protection and security.