Shred-it®

DATA PROTECTION REPORT 2019

CANADIAN EDITION

Contents

Foreword

On a global stage, Canada's business community is associated with integrity, trustworthiness, and a commitment to purpose beyond profit. It is also notoriously conservative and generally slower to adapt to changing market conditions than its American peers.

What all companies have come to learn is that ensuring information security and data protection is a business priority in today's fast-paced,data-driven environment. And while businesses, government and consumers alike acknowledge its importance, identifying gaps in data protection and determining what policies, procedures and actions need to be adopted requires a focused look at current and evolving risks and trends.

In thinking about recent drivers of data protection priorities, 2018 was dominated by the European General Data Protection Regulation (GDPR) and the implications of its compliance requirements to businesses and consumers around the world. The government of Canada also introduced updates to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) that were focused on transparency and reporting. National consultations launched by the federal government to explore "digital and data transformation", including how best to ensure Canadians have trust and confidence in how their data is being used.

With compliance and transparency defining 2018, what does 2019 hold?

More than a necessity to maintain current business reputation, data protection is being increasingly linked to business performance and competitiveness. It can be a key competitive advantage – or disadvantage, for those not developing and implementing a comprehensive data protection strategy.

It is with that lens that Shred-it presents the results of its ninth annual survey. As in the past, we sought to identify the insights, opinions and best practices of data protection among Small Business Owners (SBOs), C-Suite Executives (C-Suites) and members of the public at large from across the country to help Canadians better navigate this changing privacy landscape. Our goal is to uncover – and quantify – both the risks and opportunities Canadian businesses and consumers face, including the upsides and downsides of mishandling data and/or being breached. Just as the challenges and opportunities facing businesses evolve, so too has this report. While the previous reports were branded as the Shred-it State of the Industry Report, this year we've renamed it the **Shred-it Data Protection Report** – a name that more closely reflects the focus of the report and the value of the intelligence it provides.

This year's report provides valuable insight into potential organizational gaps for businesses – including both policies and practices – while providing guidance on developing and implementing an information security strategy that reflects the important role both businesses and employees play. As data protection requirements and best practices continue to evolve, Shred-it is working with Canadian businesses to adapt and succeed in today's globally competitive world.

Cindy Miller
C.E.O., Stericycle Inc.

Executive Summary

The ninth annual survey on the state of data protection has uncovered a concerning disconnect between attitudes and awareness levels around perceived information security threats, and the reality of those threats.

Shred-it surveyed

- 100 C-Suite Executives,
- 1,000 Small Business Owners
- 2,000 members of the general public across Canada

The results are conclusive:

Canadian businesses are in denial about the serious impact any data breach can have on their reputations and bottom lines.

Policies are up, but policing is down. While 83% of C-Suites and 57% of SBOs indicated a strong understanding of legal requirements, only **60% of C-Suites acknowledge strict adherence to known and understood policies** for storing and disposing of confidential paper documents and end-of-life electronics. For **SBOs, 49% acknowledge strict adherence to such a policy** for paper documents, with only 37% confirming adherence to policies for end of-life electronic devices.

Not only are businesses in denial, but the 2019 DPR also found that consumer trust is fragile. The current disconnect between business leaders and consumers puts businesses on a concerning path.

- **36% of Canadians stated they would lose trust in an organization following a breach.**
- **More than 1 in 4 consumers would take their business elsewhere following a data breach.**
- **Only 2 in 5 believe that all digital data breaches are disclosed.**
- **1 in 3 consumers say they would actively tell others about a breach to which they were victim.**

The data from this year's survey paints a compelling and urgent picture: the risk of a breach is increasing, but there is growing complacency in preparing for the inevitable.

47%

of C-Suites view data breaches as

not a big deal
blown out of proportion

74%

of SBOs think any breach is

A BIG DEAL

82%

of Canadian consumers agree with SBOs

The number of reported data breaches in Canada doubled in the past year:

45%

of C-Suites confirming a breach
(versus 24% in 2018)

8%

of small businesses reporting a breach
(up from 5% in 2018)

The result of the disconnect between attitudes held by business leaders and the perceptions held by consumers is worrisome, especially when taking a closer look at divergent views on the seriousness of data breaches.

As businesses of all sizes look to strengthen measures to safeguard data, employee training and compliance need to be urgent priorities, especially given the role employees play in protecting information and maintaining consumer trust.

- **52% of C-Suites and 40% of SBOs who reported a breach cited human error by employees/insiders as the main cause.**
- **Should a breach of employee data occur, 37% of employees indicated they are likely to seek employment elsewhere.**

Canada has an opportunity to become an information security and data protection leader in the global economy. Strong policies and effective compliance training and oversight are a solid foundation, but businesses cannot afford to overlook the human factor. As the 2019 Shred-it DPR shows, the biggest risk for any breach lies with employees; the biggest downside lies in lost consumer trust and loyalty. The right plan is founded in protecting both.

Shred-it is committed to being the leader in information security and helping all organizations of any size, protect their data. Through coast-to-coast service reliability, security expertise and dedicated customer experience, Shred-it helps to protect what matters to businesses.

C-Suites vs. SBOs

Canadian businesses are in denial when it comes to data protection, and unaware of the financial and reputational consequences of a material breach.

Despite the progress Canada's business community has made in strengthening data protection policies and practices, it is not enough. More needs to be done in both the largest companies and smallest businesses, and according to the results of the 2019 Data Protection Report, complacency and denial will prove increasingly costly.

While global privacy breaches and regulatory changes are making headlines around the world, protecting consumers' data – and preventing breaches – continues to be a challenge for the majority of Canadian businesses.

Volumes of information are shared across the country every day, all of it vulnerable to some kind of breach, theft or fraudulent manipulation due to an ongoing shortfall in the physical and technical safeguards being implemented by Canadian businesses. While the government's regulatory frameworks continue to evolve, businesses remain the first line of defense for Canadians' data. Their defenses are vulnerable; more must be done at the top to minimize the risk and impact of future breaches.

The insights from Shred-it's 2019 survey show that business' understanding of the legal requirements related to handling confidential information is on the rise.

83%

of C-Suites indicated a strong understanding, up from 78% in 2018,

with SBOs understanding being notably lower at

57%

a significant increase from 46% in 2018.

While those year-over-year results are good news, an understanding of requirements is only the start. Effective policies, employee training and day-to-day practices are required if confidential information is to be adequately protected.

- **Of greater concern - only 60% of C-Suites indicated strict organizational adherence to known and understood policies** for storing and disposing confidential paper documents and end-of-life electronic devices.
- **For SBOs, only 49% indicated strict adherence to such a policy for paper documents,** with a small number of SBOs confirming such practices for end-of life electronic devices at 37%.

Needless to say, an erosion of customer trust and loyalty of that magnitude would be catastrophic. Couple this with the finding that one in three (31%) consumers say that they would actively tell others about a breach to which they were victim, means one thing: **there is an urgent need for organizations of all sizes to strengthen their policies, training and practices to safeguard the data entrusted to them by Canadian consumers.**

More than **1 in 4** consumers surveyed indicated that they would take their business elsewhere following a data breach.

Here is why that matters. These figures fly in the face of the evolving context of consumer sentiment across Canada.

Data Security and Consumer Trust

The results of this year's 2019 survey point to an underlying – and significant – theme of fragile consumer trust. From the 36% of Canadians who indicated that they would lose trust in an organization following a data breach, to the finding that only 42% believe that all digital data breaches are disclosed, the reputational impact of data protection cannot be understated.

While C-Suites and SBOs recognize data security risks, they underestimate consequences, creating a worrisome disconnect. Simply put, a data breach is a trust breach, and consumers will hold those responsible to account.

Canada's business leaders need to pay attention

47%

of C-Suites respondents view data breaches as **"NOT A BIG DEAL"** and **"BLOWN OUT OF PROPORTION".**

82%

of consumers disagree and think that data breaches are, in fact, **A BIG DEAL.** This line of thinking must change.

SBOs are a little more in tune with reality, as

74%

RECOGNIZE THE SEVERITY OF DATA BREACHES, and do not agree that they are blown out of proportion.

At the same time, the number of reported data breaches in Canada doubled in the past year, with

45%

of C-Suites confirming a breach
(versus 24% in 2018)

8%

of small businesses reporting a breach
(up from 5% in 2018)

This year's DPR should be a harsh wake-up call to Canadian business leaders. Those demonstrating a complacent attitude around the seriousness of data breaches will risk taking a hit to their bottom line and suffer severe reputational damage.

Many business leaders and owners admit things are going to get worse.

66%

of C-Suites and

25%

of SBOs believe they are likely to suffer a data breach within the next 5 years.

Pay attention to Millennials

They make up the largest consumer base in Canada, and their actions will have the biggest impact on a business should an organization they support suffer a data breach. They are almost twice as likely than other demographics to...

	Millennials (aged 18-34)	**Others** (aged 35+)
Lose Trust	43%	33%
Seek Compensation	33%	18%
Tell Others	39%	29%

The Hidden Risks of Remote Work Policies

	C-Suites		SBOs	
	2019	2018	2019	2018
Over the past year, businesses of all sizes have reported an increase in remote working, with most **C-Suites and SBOs confirming the use of a flexible or off-site working model.**	95%	89%	59%	50%
Both groups agree **flexible work arrangements are likely to become increasingly important to their employees over the next 5 years.**	97%	83%	74%	66%

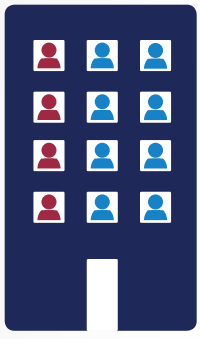
Last year's 2018 data uncovered that 74% of C-Suites and only 43% of SBOs had a policy in place for storing and disposing of confidential information at off-site locations. **This year, that number has risen – a full 96% of C-Suites confirmed such a policy is now in place, with 55% of SBOs confirming the same.** While that increase is promising, the numbers still indicate a significant blind spot for SBOs that needs to be addressed. Leaders need to remain vigilant to monitor compliance, and update policies as technologies and regulations evolve.

The Human Side of Data Protection

Given the strong correlations the 2019 DPR shows between effective data protection, consumer trust and business performance, it is critically important for employees to embrace and adhere to their employer's data protection standards. Their company's survival, and their careers, hang in the balance.

This is not an issue of leadership not trusting their staff members, as mistakes happen at all levels of any organization.

Thus, aside from ensuring policies are constantly reviewed and updated to meet evolving needs, training employees on a regular basis on what is expected of them, the role they play in safeguarding the company's data and the tools available to them to help them succeed must be an ongoing priority for both C-Suites and SBOs.



The survey also uncovered an additional reason why a priority needs to be placed on employees –

37%

indicated they are likely to seek employment elsewhere following a data breach compromising employee data at their place of employment.

52% **of C-Suites**

and

40% **of SBOs**

who reported a breach cited human error by employees/ insiders as the main cause.

One hypothesis is that a corporate data breach (and how a company responds to that breach) may be interpreted by employees as the company being equally careless with their own personal data.

The 2019 Data Protection Report reveals a clear misperception of the importance and impact of data security within businesses at all levels. Leaders acknowledge that the risk of a breach is increasing, but there is a growing complacency in preparing for the inevitable. The findings also offer a warning to be ignored at every leader's peril: consumers are starting to vote with their wallets. Lose their data and you may lose their business.

Employees vs. Employers

The main cause of data breaches? Human error.

While executives trust that their employees will prioritize and respect data protection policies, this year's survey uncovered that the majority of breaches are a result of human error. As a result, there is an urgent need to create workplace cultures that prioritize data protection and information security. The failure to do so will not only increase the risk of data loss, but also any such loss may impact customer loyalty, financial performance and employee retention.

A Concerning Gap

While the frequency of data breaches in Canada continues to grow, the 2019 DPR highlights a gap between employers (both C-Suites and SBOs) and employees, and their respective awareness, beliefs and practices regarding the disposal of physical and digital data.

It starts with varying levels of awareness – particularly among larger corporations

73%

of C-Suites indicated they are very aware of how to properly dispose of hard drives, USBs and other electronic devices

53%

feel their employees are

The gap is smaller for SBOs

44%

state they are very aware of such practices

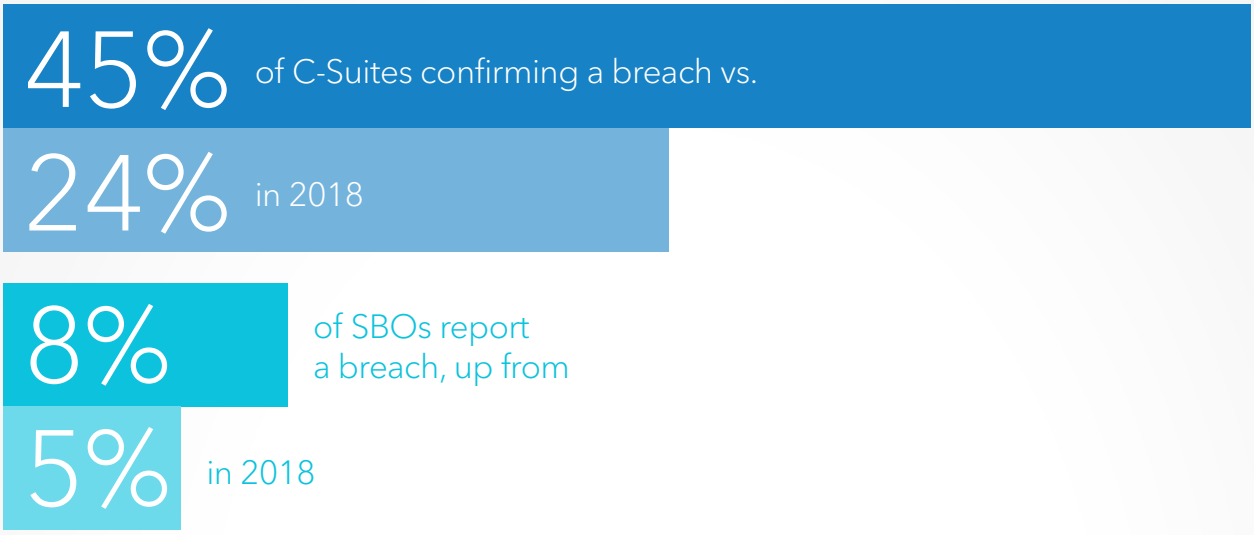
37%

feel their employees are

The low levels of awareness among all groups is surprising compared to the investment most large organizations claim they are making in training their employees on their data security protocol. Almost all Canadian C-Suites (97%) report that their business offers employee training – either once (22%) or on an ongoing basis (76%) – to help identify and prevent common cyber-attack tactics such as phishing, ransomware or other malware. SBOs cited notably lower levels of training for employees at 60%. In short, there is a disconnect – particularly among C-Suite organizations – with weak data destruction practices not matching the training investment being made.

Beyond awareness of policies, employees and employers also view the threat of a breach quite differently. While the majority of Canadian employees (58%) said they believe it is unlikely that their organization will suffer a data breach within the next five years, the reality is that the number of data beaches are on the rise.

Reported breaches in Canada doubled over the last year:



Looking ahead, with 66% of C-Suites and 25% of SBOs acknowledging they are likely to report a data breach within the next 5 years, it is important to continue the conversation with their employees in order to mitigate the risks of a data breach from occurring.

Data Protection is Everyone's Responsibility

When asked who should take responsibility for data security within an organization, a majority of respondents (59%) indicated that it should be the employees, rather than management. This further highlights the need for effective and regular employee training.

Findings from the DPR reveal that many C-Suites (42%) and SBOs (36%) who view a data breach as being likely at their organization, within the next 5 years, expect human error by an employee(s)/insider(s) to be the cause.

The Human Capital Impact

Perhaps most alarmingly, this year's survey uncovered the potential human capital impact to organizations in the event of a breach. A full one-third of working Canadians indicated they would likely seek new employment opportunities if their employer suffered a breach of customer (29%) or employee data (37%).

50%

of all C-Suites predict that human error on the part of an external vendor will be responsible for a future breach, pointing to the need to extend training to third-party partners.

Millennials are significantly more likely to abandon their organization compared to older demographics if a data breach were to occur.

	Millennials (aged 18-34)	Others (aged 35+)
Will go elsewhere if employee data is compromised	52%	30%
Would jump ship if customer data is compromised	40%	24%

The urgency with which Canada's business community must act is clear. Organizations need to foster cultures that place the utmost priority on data protection – as a compliance requirement, but also as a critical employee retention advantage.

Consumers

Consumers do not believe their personal data is safe.

Consumer loyalty comes at a price. Quality and value have always played into it. Of late, a brand's social responsibility efforts have also factored in. Shred-it's 2019 DPR adds another dimension to the loyalty equation: the safety of the personal data they entrust to the brands they choose to buy from.

More than one in four consumers (27%) surveyed, indicated that they would take their business elsewhere following a data breach, which could be devastating for a business. Further, one in three consumers (31%) say that they would actively tell others about a breach to which they were victim, which highlights an urgent need for businesses to make information security a priority.

Indeed, their survival may depend on it.

An overwhelming

50%

of Canadians feel that their personal data security has declined over the past 10 years – largely due to how easily fraudsters are able to access personal information.

Canadian businesses of all sizes must rise up to the challenge to make consumers feel secure or suffer the consequences – and those consequences are significant.

Perception is Reality

The 2019 DPR shows that consumer trust around the security of their personal data is becoming a driving force behind decision-making. In addition to data protection challenges and an increasing number of breaches, business leaders should also be concerned about something just as powerful – consumer perception.

This year's survey results highlight a real disconnect between consumer perceptions and corporate reality when it comes to the commitment and steps Canadian businesses are taking to protect their customers' data.

82%

Consumers are nearly unanimous in their belief that any breach of their personal data is a big deal

53%

In stark contrast, only half of leaders in Canada's largest corporations would put a breach in that same category

74%

The gap is much lower among SBOs, as three in four rate the impact of breaches as significant

27%

Millennials are most likely to agree that data breaches are "not a big deal"

15%

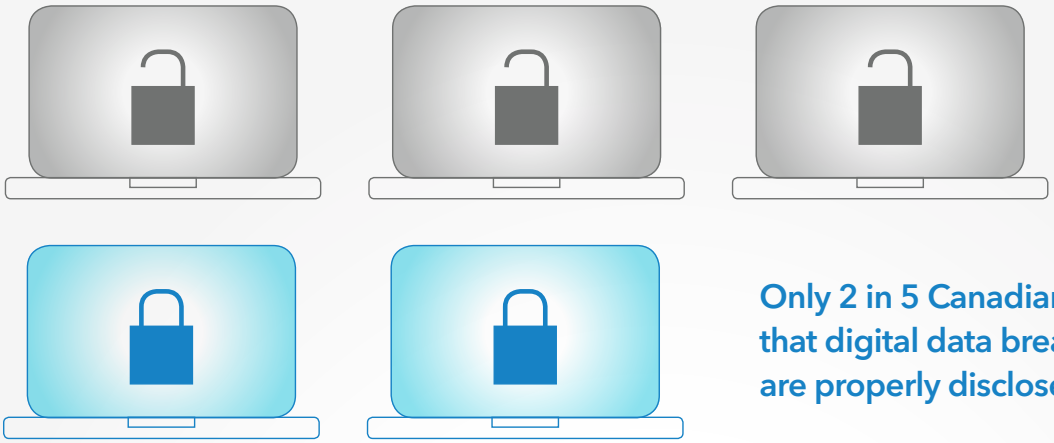
when compared to older demographics (Gen Xers and Boomers)

Perhaps this is the result of breaches becoming commonplace for the first generation to grow up in a digital world. Still, this alarming complacency among the nation's business leaders cannot go unchecked.

Rebuilding Consumer trust

Businesses of all sizes need to do more, and quickly. Consumer trust is fragile and leaders of all types of organizations must act to strengthen their data protection efforts to mitigate the erosion of consumer trust and loyalty they can expect to suffer after a breach.

Transparency has never been more important as 45% of large businesses in Canada report having been breached – a level that is up dramatically from 24% in 2018. Businesses need to walk the talk. **Consumers expect more.**



Only 2 in 5 Canadians trust that digital data breaches are properly disclosed.

Findings from the 2019 DPR tell a compelling story: businesses must act to strengthen their physical and digital data protection policies, while improving training and compliance oversight.

Ensuring consumers have visibility into and an understanding of those policies and practices is becoming just as important, as consumers' perception of how their data is – or is not – being protected, can be just as powerful as reality.

By being consumer-centric and elevating the role of data security across an organization, businesses can strengthen consumer trust, corporate reputation and competitiveness.

27%

claim that they are prepared to vote with their wallets by **taking their business elsewhere** if a business they currently support suffers a data breach.

Industry Specific Insights

Concerning trends across some of Canada's leading industries: **Risk, Denial and Trust.**

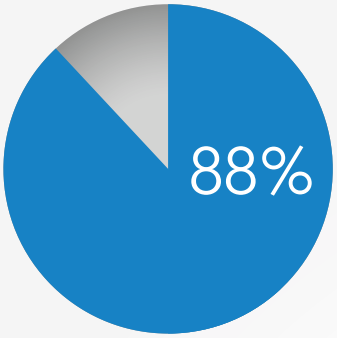
The 2019 DPR included an in-depth look at industry-specific data protection practices, across hospitality, legal and financial services, education and healthcare industries. **While business leaders in each sector face unique challenges and opportunities, the data revealed that risk, denial and trust are common themes.** Leaders of Canadian companies, large and small, must move with urgency to strengthen the ways their organizations approach information security.

The degree to which human error or accidental loss by external vendors are driving breaches in Canada is alarming.

When asked about steps being taken to ensure physical and digital information is being properly disposed of, business leaders acknowledged they are not taking appropriate measures or implementing the right policies and compliance oversight. As a result, the future of their business is at risk.

Hospitality

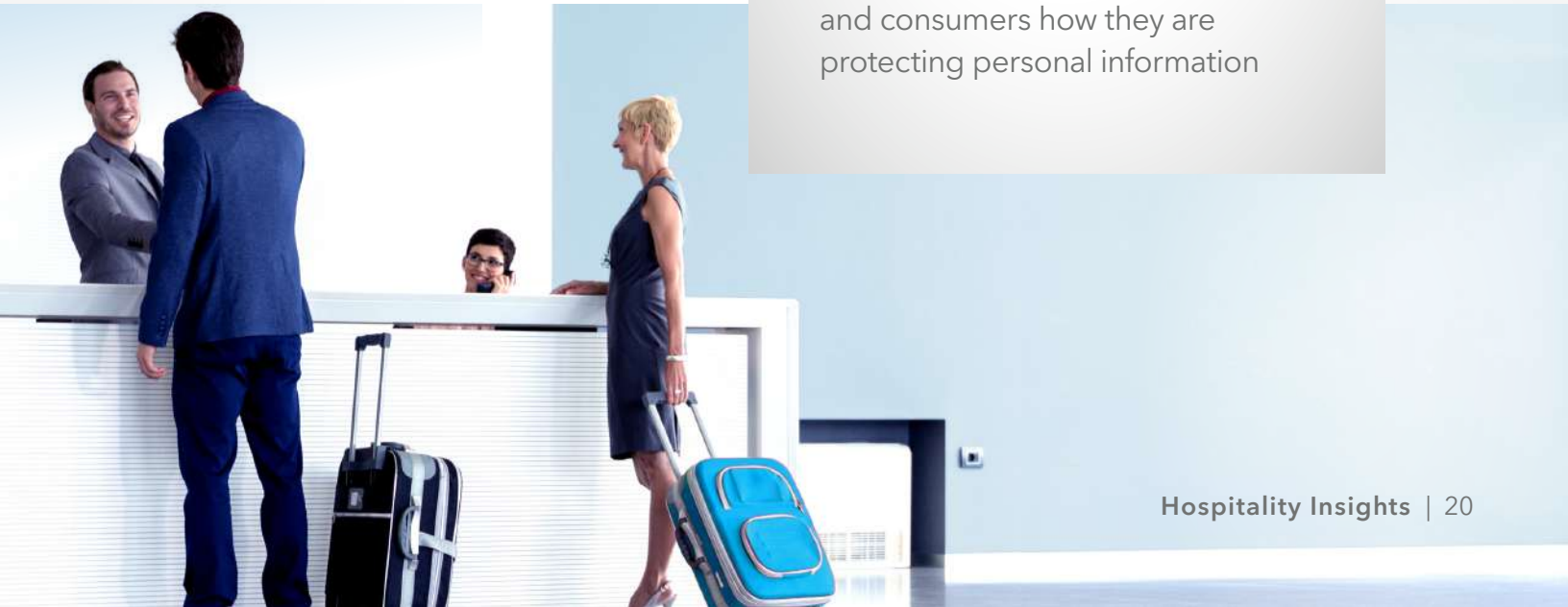
The research uncovered that the priority for hotel owners is better training for their staff. With the amount of personal and confidential information that guests travel with (i.e. passports, boarding passes etc.), hotels need to ensure that proper employee training is being done in order to mitigate potential information security risks and ensure that guests feel safe and secure during their stay.



OF HOTEL OWNERS prioritize digital data security, leaving physical document protection neglected.

Key 2019 DPR Findings

- Despite the fact that the majority (76%) of hotels have a policy for disposing of confidential paper documents, as many as 1 in 4 perceive their employees as being unaware that such a policy exists
- Only 39% of hotel owners confirm that their policy for storing and disposing of confidential information on end-of-life electronic devices is strictly adhered to
- 96% of hotel owners feel like they need to do more to show employees and consumers how they are protecting personal information

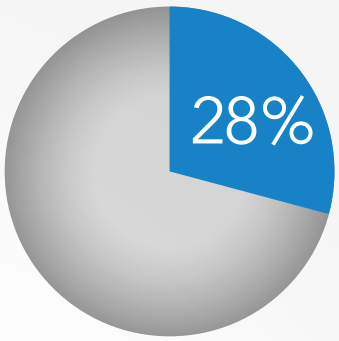


Legal & Finance

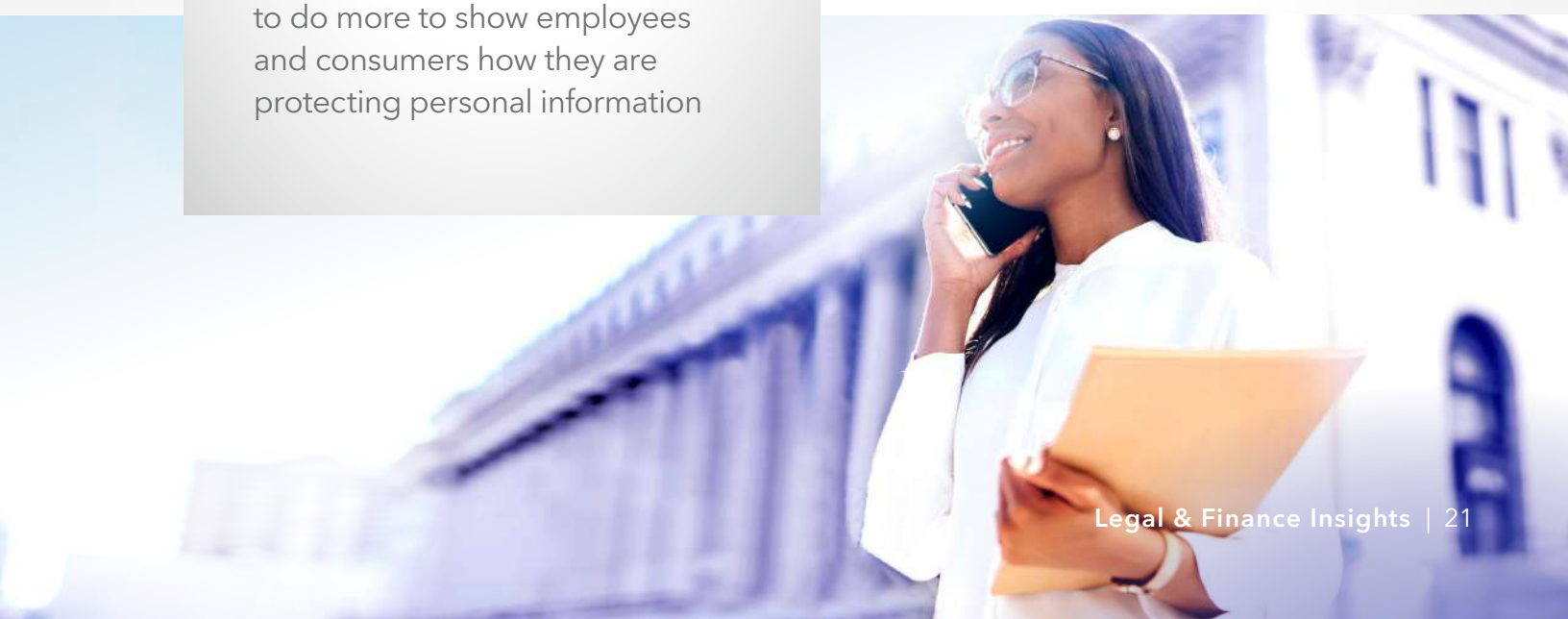
Lawyers, bankers and auditors make missteps, too. With the amount of confidential information collected, both law firms and accounting firms need to recognize that insufficient internal security protocols put their business at an increased risk. Human error – and not cybersecurity – is the leading cause of data breaches in their sectors. As a result, there is a need to better train their associates and partners on the importance of physical information security or face the risk of client loss and/or negative reputational consequences.

Key 2019 DPR Findings

- Only 57% of legal and financial professionals believe that their policy for storing and disposing of confidential information when employees work off-site is strictly adhered to
- A quarter fear that their clients will stop doing business with them if a data breach were to occur
- 90% of both legal and financial professionals feel like they need to do more to show employees and consumers how they are protecting personal information

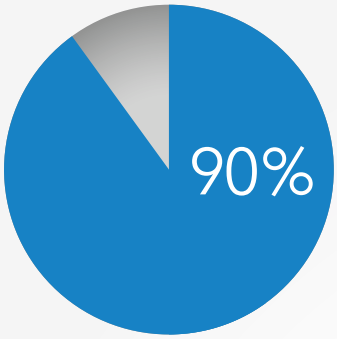


OF LEGAL AND FINANCIAL PROFESSIONALS train their employees on information security procedures twice a year or more frequently.



Education & Healthcare

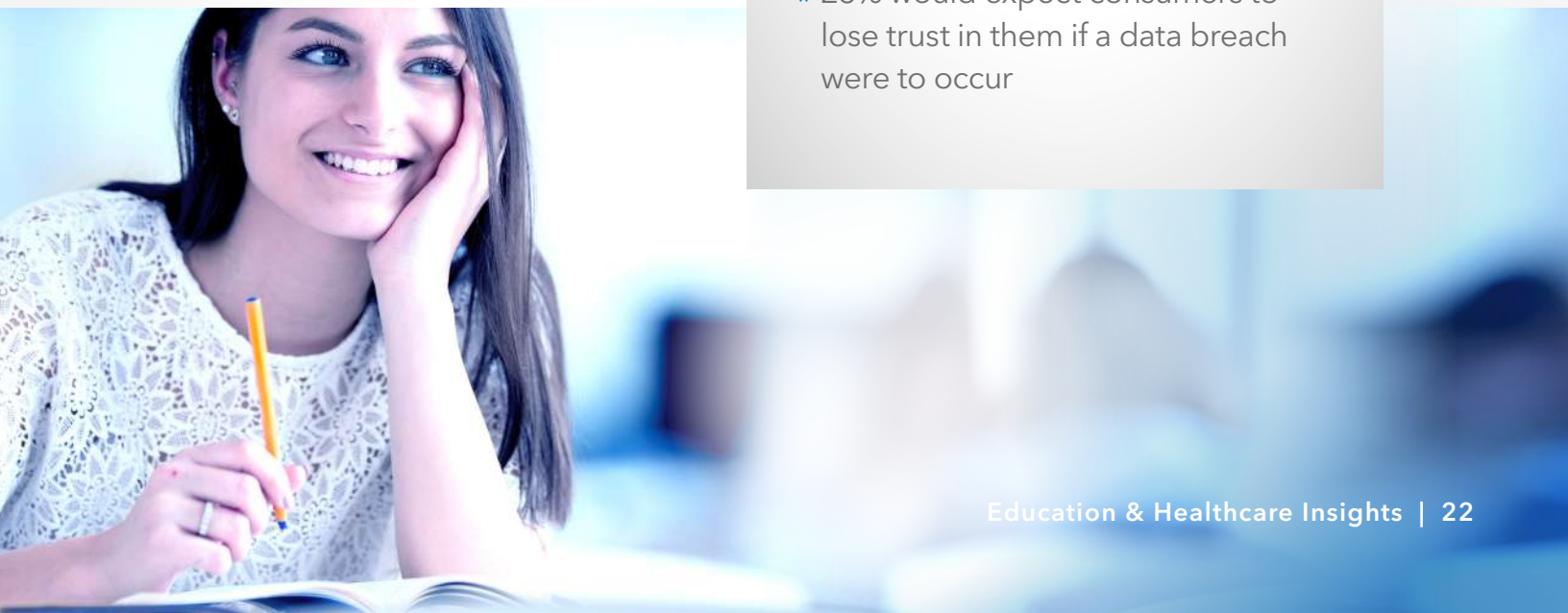
As part of the professional code of conduct, doctors have a responsibility to ensure that their patients medical information remains protected. Similarly, teachers and those in academia must also take the proper precautionary steps to ensure that students' personal information remains confidential. These institutions must not underestimate the importance of externally communicating (and demonstrating) commitment to information security.



EDUCATION AND HEALTHCARE PROFESSIONALS feel like they need to do more to show employees and consumers how they are protecting personal information.

Key 2019 DPR Findings

- 34% of educational and healthcare professionals confirm that no policy exists within their organization when it comes to storing and disposing of confidential information on end-of-life electronic devices
- Only 16% of education and healthcare professionals train their employees on information security procedures at least twice a year or more frequently
- 28% would expect consumers to lose trust in them if a data breach were to occur



Ask the Expert

A Global Perspective on Data Protection and Security

Prepared by Ponemon Institute

We live in a world that has grown increasingly dependent on information, in which access to good, reliable data has become essential for global economies. But at the same time, we are experiencing unprecedented increases in data breaches and compromised information security. The types of threats facing organizations are constantly evolving, challenging the ability of organizations to reduce the likelihood of a data breach or a security exploit. Just as alarmingly, these breaches are costly to remediate and can result in the loss of customer loyalty and the inability to retain employees.

Consumers worry about the privacy and security of their personal information and this should motivate organizations to improve their security posture. People are becoming more and more concerned about the privacy and security of their personal data for several reasons. In addition to the risk that their personal information may be compromised in a data breach, people also cite government surveillance and the growing use of mobile and connected devices as their reason for feeling less secure.

The negligent employee or contractors are the weakest link in the security chain. As you can see from the findings in this report, threats from employees, negligent or malicious, are increasingly cited as the biggest threats to an organization's information security and workplace privacy.

Knowledge is the path to protection.

" I was pleased to be asked to contribute to the 2019 Data Protection Report. As a leader in information security research, the Ponemon Institute likes to partner with brands, like Shred-it, that are thought-leaders in the industry. It is only with a clear understanding of the changing practices, perceptions, and potential threats to privacy and confidentiality can organizations take the right steps toward protecting their valuable information."

Larry Ponemon, Ph.D., Chairman and Founder, Ponemon Institute

Predictions About Global Data Protection and Security.

Companies are embracing the digital economy because it enables connectivity to more users, devices and data than ever before.

From a business perspective, it means making decisions based on market demand and business opportunity, empowering consumers and fostering collaboration through innovation (mobile, cloud, IoT) and quickly and effectively releasing new applications to drive growth. Organizations believe digital transformation improves consumer and customer interactions.

The rise of nation-state attacks.

State-sponsored attackers go after high-value information that will give their countries a competitive and military advantage, such as intellectual property, classified military information, schematic drawings, etc. They are motivated more by strategic than financial gain. Organizations are finding it difficult to differentiate between nation-state attacks and other types of cyberattacks. Nation state attacks prey upon standard business practices and target employees in business units, who are untrained or unaware of most security practices. For example, many nation state attacks have attempted to infiltrate a network through the HR Department, using resumes submitted as attachments laced with malware.

More organizations will recognize the value of artificial intelligence (AI).

AI can have a very positive impact on an organization's security posture and bottom line. The biggest benefit is the increase in speed of analyzing threats followed by an acceleration in the containment of infected endpoints, devices and hosts (64% of respondents).

As the threat landscape worsens, organizations will increasingly rely upon the expertise of the CISO.

According to Ponemon Institute research, IT security practitioners believe their responsibilities will not be limited to the IT function and will evolve in importance and span of control.

Cybersecurity governance practices are expected to improve.

More senior IT security leaders will require frequent audits and assessments of the effectiveness of their security policies and procedures to protect their most sensitive and confidential data assets.

Companies will invest in enabling security technologies and managed security service providers as part of their cybersecurity strategy.

Technologies expected to increase in importance are threat intelligence feeds and analytics in cyber defense. It is predicted that more companies will invest in big data analytics, threat intelligence sharing and the engagement of managed service providers.

Companies are expected to improve collaboration and reduce the complexity of business and IT operations.

Companies will be more successful in reducing the complexity of their business and IT operations. Organizational barriers such as a lack of cybersecurity leadership and a lack of collaboration among the various functions are expected to improve.

Information security needs to be looked at holistically.

With the onslaught of cyber-attacks and rise in digital hacks, it is easy to forget the confidential and personally identifiable information found on paper documents. Organizations need to start thinking of information security in its broadest sense, ensuring not only the safety of their digital assets while simultaneously taking active measures to ensure document security, too.

A Turning Point for Canadian Business Leaders

Shred-it's 2019 Data Protection Report provides Canadian business leaders with an opportunity. The data confirms that businesses, large and small, place a vital importance and improving their existing approach to data protection. Businesses must do their due diligence and review and revise current policies and procedures in order to increase satisfaction and confidence among their key stakeholders, including both customers and their own employees. This requires additional investment in employee training, increased assurance to customers that data protection is a priority and implementing physical safeguards.

The importance of data and how it is increasingly being used to make business decisions will not go away any time soon. In fact, the collection and processing of customer data will only increase with time. As recent news events confirm, even the world's largest brands are vulnerable to the consequences if they violate their customers' trust.

Throughout the 2019 DPR, three prominent themes emerged:

- a growing sense of denial among business leaders that information security is a real concern;
- a growing risk among every company's employee base that breaches could impact retention; and
- a growing willingness amongst the general public to hold any company suffering a breach accountable.

This should be a wake-up call to Canadian business leaders. Complacency will lead to breaches, and breaches will cost them – not just in reputation, but in sales, profits, employee retention and more.

There are two other notable key findings from the 2019 DPR. First, human error - rather than outside sources - are an organization's biggest threat when it comes to data protection. Second, millennials, Canada's largest consumer and workforce pool, and ultimately, a group that has the ability to impact your bottom line, will take their business elsewhere following a data breach.

These threats are real, and regardless of the industry, all organizations must take action. Those that do not, run the risk of damaging their reputation. As businesses and modern workplace trends continue to evolve, data protection practices must evolve with it. The competitiveness of a business depends on it.

The good news is that there are tangible solutions that businesses can incorporate into their operations. Tougher information security and data protection policies, better training and ongoing policing are all part of the solution. So, too, is ensuring the entire organization knows what data to keep, what data to destroy, and how to do each without risk. Shred-it has the expertise and experience to be part of your solution, and our people are committed to helping you protect and safeguard your data, your reputation and your business.

Information has never been more valuable. And the need to protect it? Never more important.

Choose the information security partner who can help you meet the growing information security challenges facing your organization. With industry-leading information security services, Shred-it helps protect your reputation, your revenue, and your business.

Security Expertise

With 30 years of destruction expertise, an end-to-end secure chain of custody, our primary focus on document security ensures your confidential information remains confidential.

Service Reliability

Whether you are a large-scale national enterprise or one of thousands of small businesses, you can put the power of the largest shredding fleet and the largest service footprint in North America to work for you.

Customer Experience

From a range of self-service options and customizable destruction solutions to responsive, dedicated, customer service support, Shred-it is 100% committed to your protection.

We protect what matters.

Learn more about information security and how Shred-it can protect your organization at **shredit.com** or call **800-697-4733** today.

About the 2019 Data Protection Report

Shred-it commissioned Ipsos to conduct a quantitative online survey of two distinct sample groups: Small Business Owners (SBO) in Canada (n=1,000) with fewer than 100 employees. C-Suite Executives in Canada (n=100), with a minimum of 100 employees. Data for Small Business Owners is weighted by region. Data for C-Suite Executives is unweighted as the population is unknown. The precision of Ipsos online surveys is calculated via a credibility interval. In this case, the Canada SBO sample is considered accurate to within +/- 3.5 percentage points had all Canadian small business owners been surveyed, and the Canada C-Suite sample is accurate to within +/- 11.2 percentage points had all Canadian C-Suite Executives been surveyed. The fieldwork was conducted between March 26th and April 1st, 2019.

In addition to the quantitative online survey, Ipsos conducted a short omnibus survey among a gen pop sample of n=2,002 Canadians about data protection and security. The results of the omnibus survey have been reported separately, though comparisons against relevant questions of interest have been included in this report. The credibility interval for this sample group is +/- 2.5 percentage points, 19 times out of 20, of what the results would have been had all adults in Canada over the age of 18 been surveyed.

Info Security Products Guide 2019 GLOBAL EXCELLENCE GOLD ★★★★★

Shred-it®