DATA PROTECTION REPORT 2021

No Longer Optional: Invest in Data and Information Security Now or Pay Later

We protect what matters.

Shred-it®
A Stericycle® Solution

Table of Contents

Foreword

If ever there was a year that underscored the deepening importance of investing in secure document management, digital data protection, and information security, 2021 is it.

COVID-19 has reshaped the way we work and where we work, putting stress on systems, partnerships, and networks. Though high-profile cyber breaches get the most media attention, disclosed physical breaches—including document theft—still accounted for 43% of breached assets in 2021.[1]

It is critical for business leaders across industries to recognize that keeping a low profile will no longer cut it. They must understand the high stakes at play and the implications of inadequate data protection, not only to protect their business performance, sales, and share price, but also to safeguard their reputation and retain customers. They must also prioritize efforts to plan for new and emerging threats—inside and outside their walls. Additionally, with the majority of states currently working on comprehensive consumer privacy bills, businesses must stay informed on changes in data protection legislation to ensure compliance. Savvy leaders will leverage these unprecedented times as an opportunity to promote trust and build a new kind of customer relationship by prioritizing information security.

In support of its mission to help organizations protect the world's confidential information and prevent data breaches, Shred-it, a Stericycle solution, has drawn on detailed findings from an in-depth survey of C-level executives, small and medium business owners, and consumers across North America to produce its 11th annual Data Protection Report (DPR). As the industry leader in secure information destruction, we're committed to protecting the health and well-being of our clients' trusted relationships, brand reputation, and bottom line. The 2021 DPR was developed to offer practical insights and recommended next steps—beyond a mere accounting of survey findings.

To our 2021 survey contributors, thank you. You understand that no one is immune from the threat of a data breach, and your insights serve as a powerful reinforcement of the importance of information security—to protect your data, reputation, and businesses. To our readers, know that Stericycle, through our Shred-it secure information destruction solution, is in the fight with you. Our team stands by, ready to help navigate the intricacies of the ever-changing data protection landscape to shape a healthier and safer world for everyone, everywhere, every day.

S. Cory White
Executive Vice President and Chief Commercial Officer | Stericycle

Key Takeaways from the 2021 Report Reveal:

- With Increasing Regulations and Financial Risk, Keeping a Low Profile Won't Cut It
- Data Security Reputation Plays a Crucial Role in Consumer Perspectives and Behaviors
- Insider Threats Continue to Loom, and Businesses Need to Be Vigilant

Executive Summary

Data protection laws and regulations have evolved over the past 10 years to better protect consumer data and encourage businesses to take action—and more changes are on the horizon. Several states, such as California, Colorado, and Virginia, have recently implemented consumer privacy legislation, and more are expected to follow as a majority of states are working on comprehensive consumer privacy legislation. In addition, Canada has already enacted the Personal Information Protection and Electronic Documents Act.

While the financial impact of a data breach overall is potentially great, the cost of non-compliance is a leading contributor.

> **According to IBM's 2021 Cost of a Data Breach Report,[2] "out of a selection of 25 cost factors that either amplify or mitigate data breach costs, compliance failures was the top cost amplifying factor."**

In addition to regulatory action and fines as well as legal fees, data breaches can also have a devastating impact to a business's bottom line—including declining brand reputation and the loss of customers. Given the ramifications associated with data breaches, it is important to understand how a data breach may occur and how businesses can best prepare themselves. Data breaches fall into two primary categories, physical and digital. **Physical breaches** include the theft of items or equipment such as employee files, tax filings, customer information, and medical records. **Digital breaches** are comprised of unauthorized access, system or human error, or a deliberate attack on a system or network.

Physical Breach

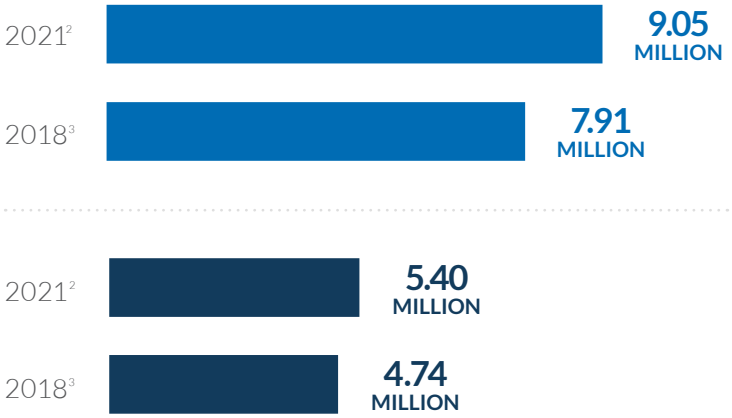
PAPER DOCUMENTS | LAPTOP COMPUTERS | EXTERNAL HARD DRIVES

Digital Breach

MALWARE | RANSOMWARE | PHISHING

Average Cost of a Data Breach Has Grown Notably Since 2018

(Measured in U.S. $ millions) — U.S. — CANADA



More than **50%** OF **STATES** are expected to implement consumer privacy legislation[4]

Key Insights

Based on in-depth 2021 survey data and analysis of North American business leaders and consumers, Shred-it's 2021 DPR reveals critical insights on the ever-evolving information security landscape. This year's report delivers straight forward, practical recommendations for business leaders on the front lines of the battle to keep their data secure, highlighting the following key themes:

- **The Incidence of a Data Breach Is Likely to Occur, and Businesses May Not Be Prepared**
  Approximately four out of 10 business leaders rate the risk of an attempted data breach in the next 12 months as a '4' or '5' on a 5-point risk scale, with '5' being the highest risk. This may leave businesses unprepared, as more than half of businesses surveyed don't have an incident response plan.

- **Data Security Reputation Plays a Strong Role in Consumer Perspectives and Behaviors**
  Consumers continue to take their personal information security very seriously. Over 80% of consumers decide who to do business with based on a company's reputation for data security.

- **Insider Threats Continue to Loom**
  While malicious outsiders are sources of data breaches, in many cases, 'trusted' insiders—external partners (40%) and employee error (22%)—are as likely to have been the cause. This highlights the need for businesses to have preventative measures in place for all data sources.

Survey Respondents Comprised Of:


C-level Executives


Consumers


Small and Medium Busines Owners

ACROSS FIVE INDUSTRIES:


Healthcare


Finance


Professional Services


Insurance


Real Estate

Investing in Data and Information Security Can No Longer Be Considered Optional

4 OUT OF 10 BUSINESS LEADERS
rate the risk of an attempted data breach in the next 12 months as a '4' or '5' on a 5-point risk scale

More than **50% OF BUSINESS LEADERS**
don't have an incident response plan

Over **80% OF CONSUMERS**
decide who to do business with based on a company's reputation for data security

40% OF DATA BREACHES
are caused by external partners
AND NEARLY **25%**
by employee error

WITH INCREASING REGULATIONS AND FINANCIAL RISK

Keeping a Low Profile Won't Cut It

With the high probability that businesses will experience a data breach, it is essential that they prepare themselves before the breach occurs. Complacency will not work, as no organization is immune. It doesn't matter if you are dealing with electronic or paper data, the risks are the same. In the past, maintaining a low profile allowed some organizations to get by. That is no longer the case as everyone creates data—and with data, they become a target.

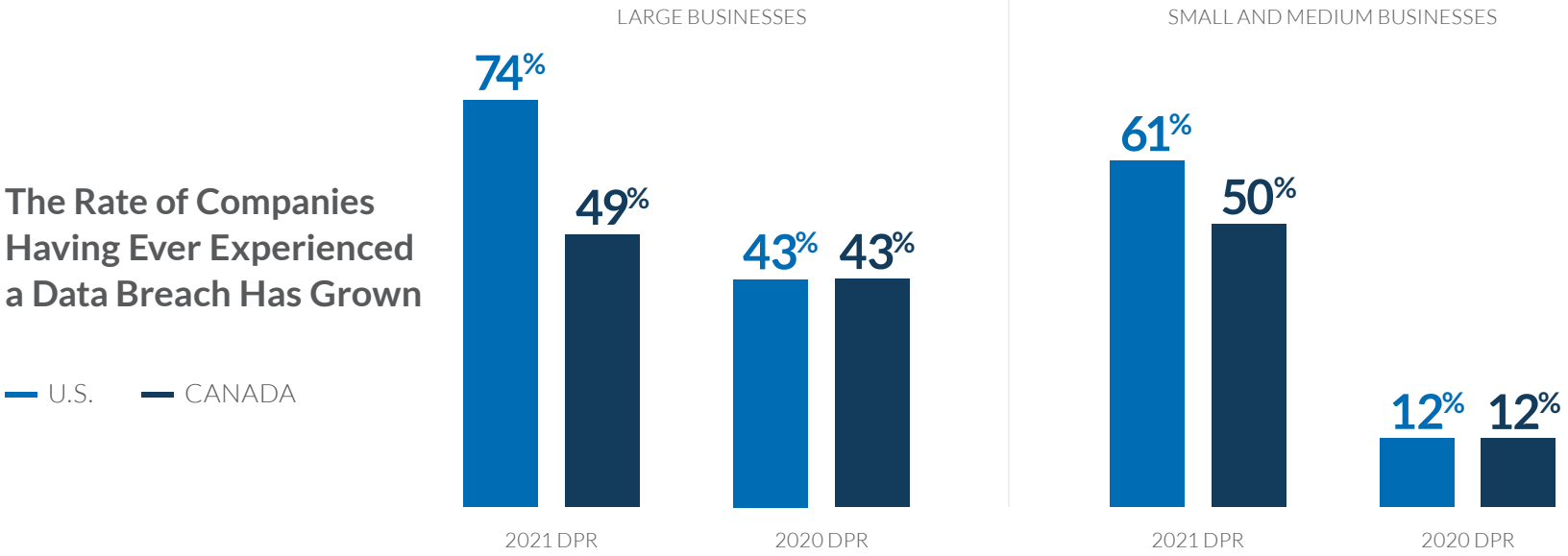
The Incidence of Data Breaches Continues to Grow

Findings from this year's DPR indicate that three-quarters of large businesses in the U.S. who were surveyed have ever experienced a data breach, as well as more than half of small and medium-sized businesses surveyed in the U.S. This is a significant increase from the 2020 DPR. While not as prevalent as in the U.S., large businesses in Canada also saw an increase in having ever experienced a data breach.

According to Risk Based Security's 2020 Year End Report, in 2020 more than 37 billion records were exposed to thousands globally—a 141% increase compared to 2019.[5] This doesn't bode well for North American businesses as 1 in 4 fear that an attempted data breach is very likely for their company in the next 12 months.

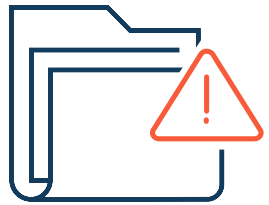
While cyberattacks make headlines, physical data breaches are a concern as well. A recent report from Verizon shows that physical breaches with known data disclosure accounted for 43% of breached assets.[1]

The Rate of Companies Having Ever Experienced a Data Breach Has Grown



In 2020,

37



BILLION RECORDS

were exposed to thousands globally—a 141% increase compared to 2019[5]

We protect what matters.

Impact of Data Breaches Too Large to Ignore

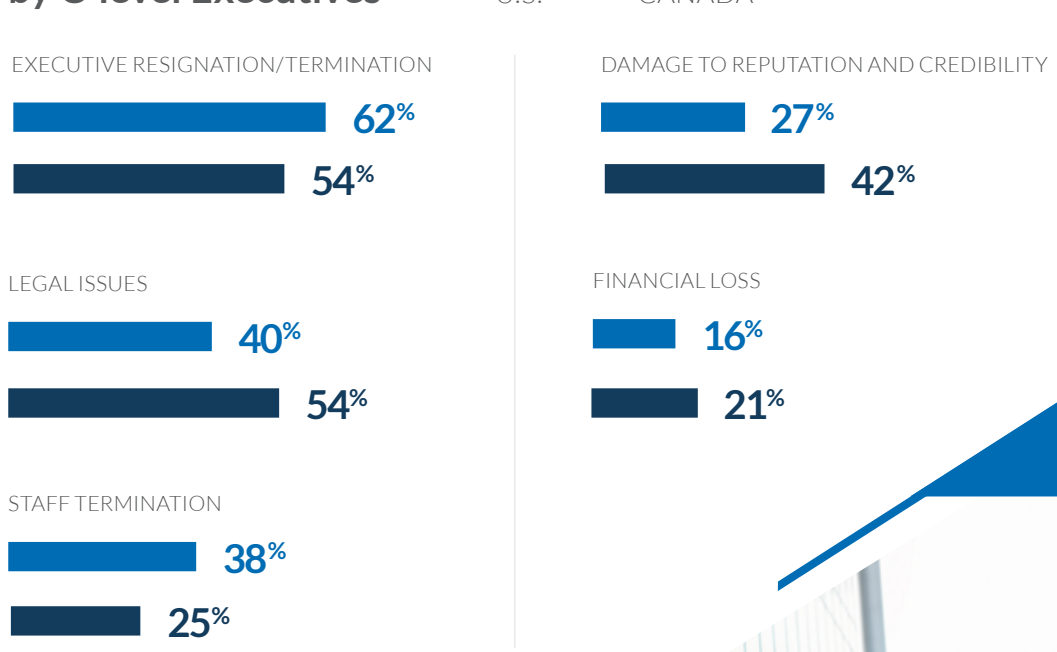
While consumer privacy violations certainly are cause for businesses to take notice, there are other significant consequences when a data breach occurs. Among North American leaders of large businesses, executive resignation or termination and legal issues were the most cited consequences.

In addition, leaders of large businesses in Canada were more likely (42%) to cite damage to their reputation and credibility as compared to their U.S. counterparts (27%).

27% OF **U.S. LARGE BUSINESSES** AND **42%** OF **CANADIAN LARGE BUSINESSES**

surveyed cite damage to their reputation and credibility as a result of a data breach

Consequences of Data Breaches as Indicated by C-level Executives



We protect what matters.

Businesses Lack Adequate Planning, Exposing Them to Risk

Many of the businesses surveyed indicated that they don't have an incident response plan (C-level: U.S. 63%, Canada 58%; SMB: U.S. 67%, Canada 57%). This proves problematic for responding quickly when a data breach occurs.

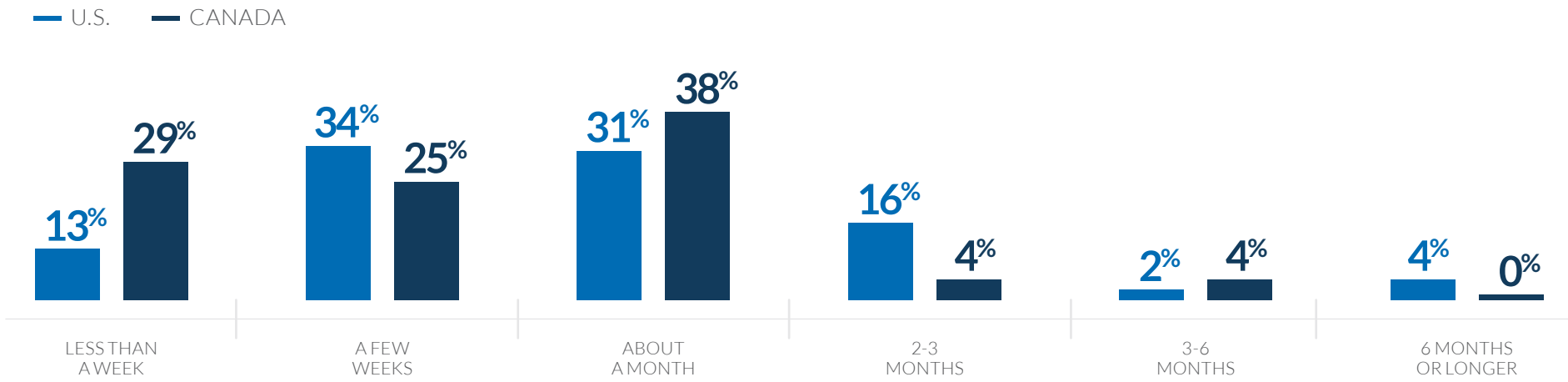
> **While many North American business leaders resolve the issues created by a data breach within a month, a few take longer—even up to six months or more.**

When the estimated cost of a data breach is $13,786 per day,[1] it is imperative that businesses have an incident response plan and remediate quickly.

63% OF **U.S. C-LEVEL BUSINESSES** AND **58%** OF **CANADIAN C-LEVEL BUSINESSES**

surveyed indicate they do not have an incident response plan

Length of Time to Resolve Issues Created by a Data Breach as Indicated by C-level Executives



We protect what matters.

DATA SECURITY REPUTATION

Plays a Crucial Role in Consumer Perspectives and Behaviors

While the financial implication of a data breach is significant, loss of consumers and their loyalty also pose a major threat to a business's bottom line. Consumers have set expectations around how their data should be handled and will go elsewhere if their expectations are not met. Maintaining consumer trust and loyalty is essential.

Consumers Continue to Be Concerned about Their Confidential Data Remaining Private

Consistent with findings from past DPRs, consumers continue to take their personal information security very seriously. Over 80% indicate an extremely high level of importance (U.S. 88% and Canada 90%). In addition, 1 in 3 North American consumers indicate that companies fall below their expectations for timely, transparent communications regarding data leaks.

Consumers have good reason to be concerned. This year's survey found that while Canadian consumers (38%) fare better, nearly 7 in 10 U.S. consumers (69%) indicated that they have been personally impacted by a data breach. This appears to be a growing trend, as the 2020 DPR showed that 53% of American consumers believe their personal data and information are less secure than they were ten years ago.

When asked to provide their perspective on why businesses do not meet their expectations in protecting their personal data, consumers said:

> **"Too many breaches and attacks come to light only when the company gets caught or is forced to reveal the breach."**

> **"Companies really don't care about personal data until it gets leaked."**

Nearly

70% OF **U.S. CONSUMERS**

surveyed have been personally impacted by a data breach in 2021, as compared to **53%** in 2020

Over

80% OF **CONSUMERS**

surveyed indicate an extremely high level of importance in personal information security

Consumers Will Act If Their Data Is Compromised

Also consistent with the findings in the 2020 DPR, consumers will take action if their data is compromised. A majority of consumers surveyed (U.S. 82% and Canada 83%) decide who to do business with based on a company's reputation for data security.

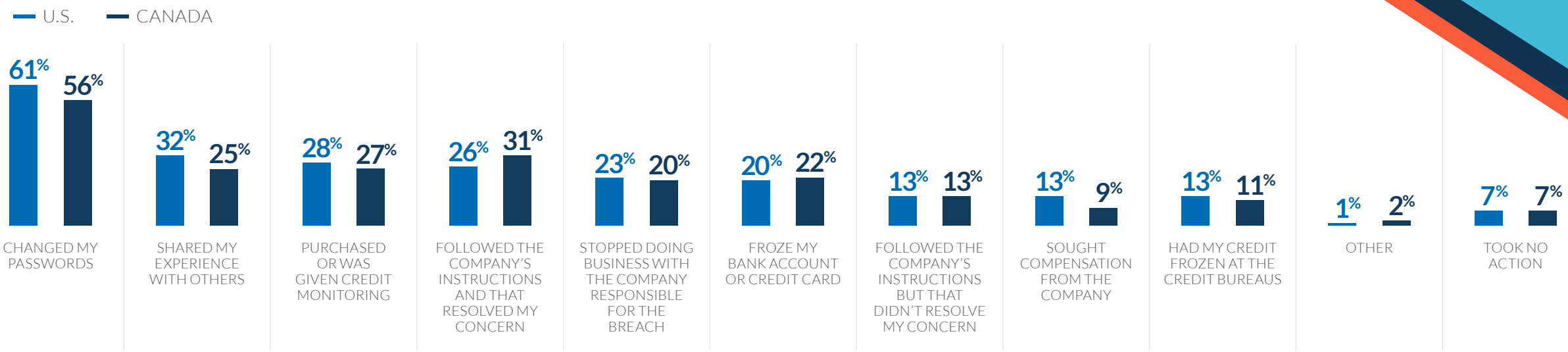
In addition, a 2020 Customer Experience Trends Report from Zendesk,[6] shows that approximately half of consumers will switch brands after one bad experience—and after more than one bad experience, that number increases to an alarmingly high 80% that would switch brands. And it doesn't end there.

> **Approximately 3 in 10 consumers (U.S. 32% and Canada 25%) will share their experience with others and nearly 1 in 4 (U.S. 23% and Canada 20%) will stop doing business with the company responsible for the breach.**

This is in line with 2020 data, where 29% shared their experience with others and 24% stopped doing business with the affected company.

Nearly **1 IN 4 CONSUMERS** surveyed stopped doing business with the company responsible for the data breach

Actions Consumers Take After a Data Breach



INSIDER THREATS CONTINUE TO LOOM

and Businesses Need to Be Vigilant

When it comes to information security, employees can be both a company's greatest strength and its greatest weakness. Malicious actors are getting more sophisticated and harder to spot, and without the proper knowledge, employees and vendors are susceptible, leaving businesses vulnerable. As a result, businesses must ensure they are vigilant at all levels or face the consequences.

‘Trusted’ Insiders Likely to Be the Source of a Data Breach

With the option to select all that apply, businesses indicate that data breaches stem from a variety of sources. The presence of malicious outsiders (55%) continues to present a threat to the information security of both large and small businesses in North America. As well, there is an alarming number of ‘trusted’ insiders who are the source of data breaches.

In the U.S., these would include breaches caused by malicious insiders (53%), external partners (40%), and employee error (22%). This is up from last year’s 2020 DPR that showed 1 in 4 c-suite executives citing social engineering scams and 1 in 5 citing external threats from vendors or contractors, as well as 1 in 5 citing physical loss or theft of sensitive information.

In 2021,

53% OF

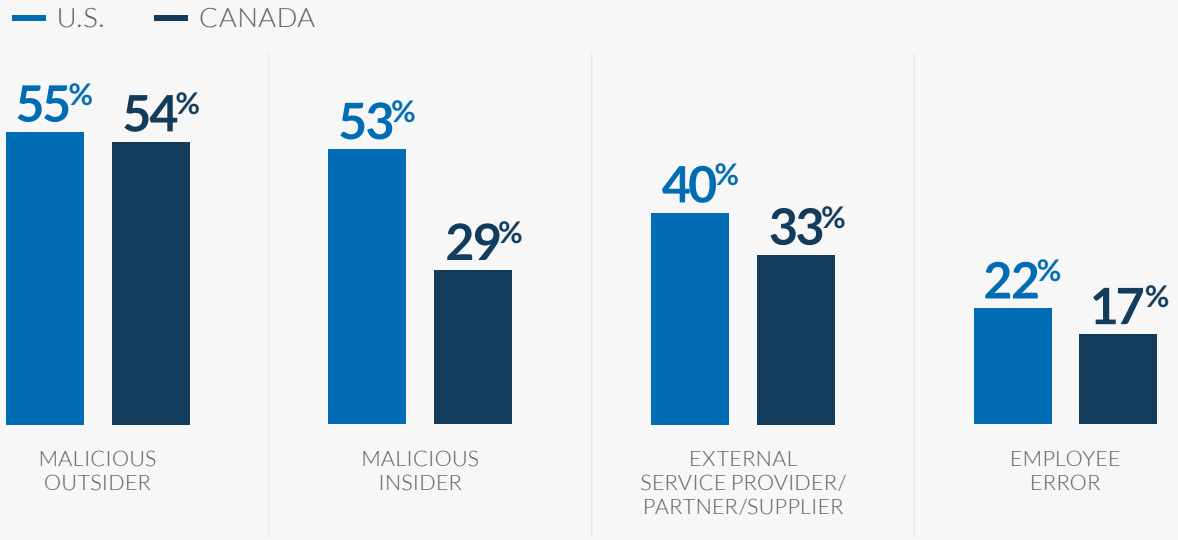
DATA BREACHES

were caused by malicious insiders

The COVID-19 pandemic has also made it more challenging for some companies to manage information security.

Nearly 30% of U.S. and 41% of Canadian small and medium-sized businesses indicated that the pandemic has made it harder to protect data. In addition, approximately 7 in 10 indicate they have a concern regarding employee adherence to the company’s privacy policies during the pandemic.

Source of Data Breaches as Indicated by C-level Executives



Businesses Indicate the Importance of Destroying Sensitive Materials, Yet Likely Do Not Have a Paper Shredding Service

Despite indicating the importance of destroying sensitive materials when they are no longer needed as a way to protect themselves, companies are least likely to mention they have paper shredding services—arguably one of the easier methods to address security vulnerabilities.

Remote work also continues to impact security threats—with over half of employees surveyed working off-site, 63% of U.S. and 45% of Canadian employees regularly print work documents.

> **Of those printing documents off-site, 1 in 4 simply dispose of them in the trash or recycle them, potentially putting their business at risk of an information security breach.**

However, a separate Shred-it survey found that 56% of businesses are interested in a service that provides document destruction combined with training and policy consultation. These can be critical for any size company looking to build both electronic and paper-focused safeguards. In addition, a majority of businesses (approximately 90%) agree environmental sustainability is a top factor when deciding which business to partner with.

56% OF BUSINESSES

are interested in a service that combines privacy and information solutions with document destruction

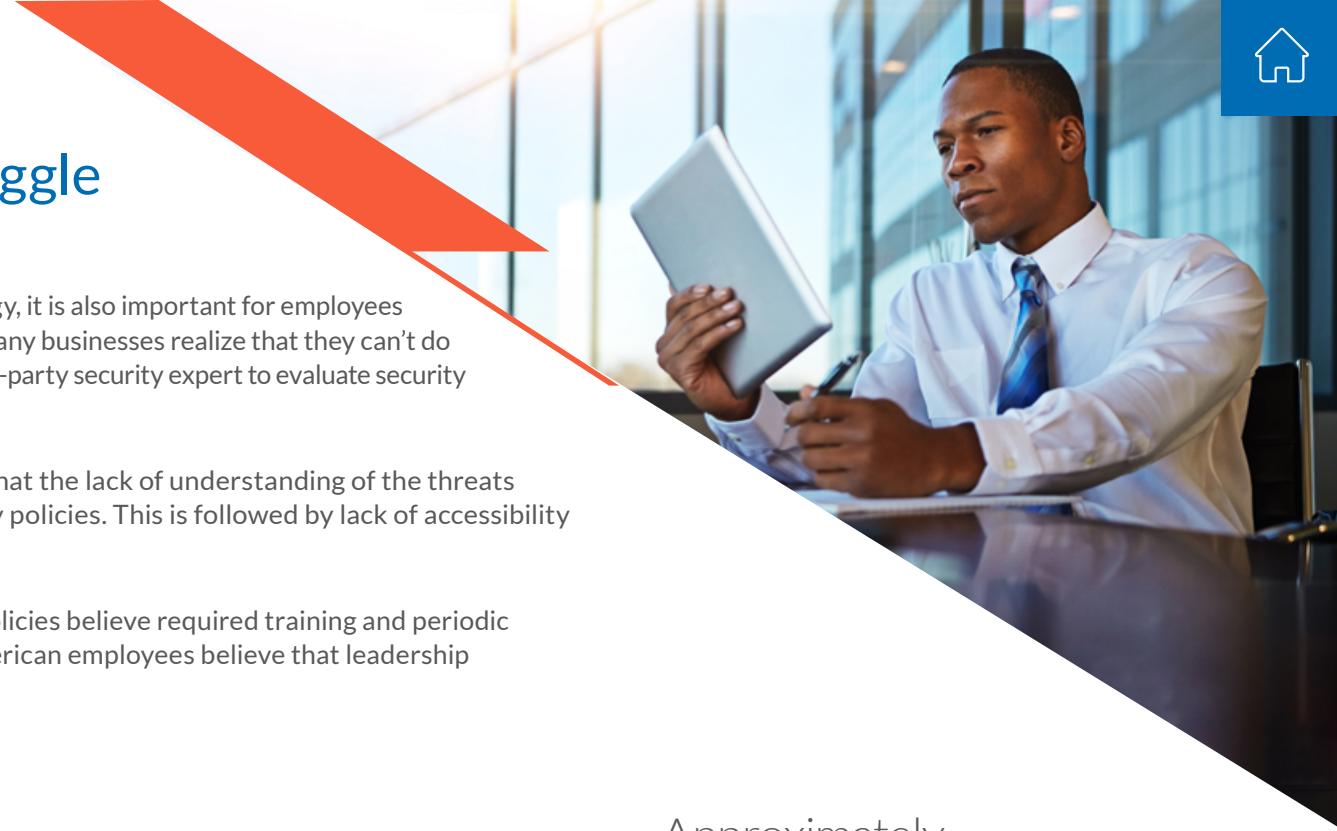
Approximately

90% OF BUSINESSES

agree that environmental sustainability is a top factor when deciding which business to partner with

25% OF EMPLOYEES WORKING OFF-SITE

dispose of printed documents in the trash or recycling bin despite potentially containing private information



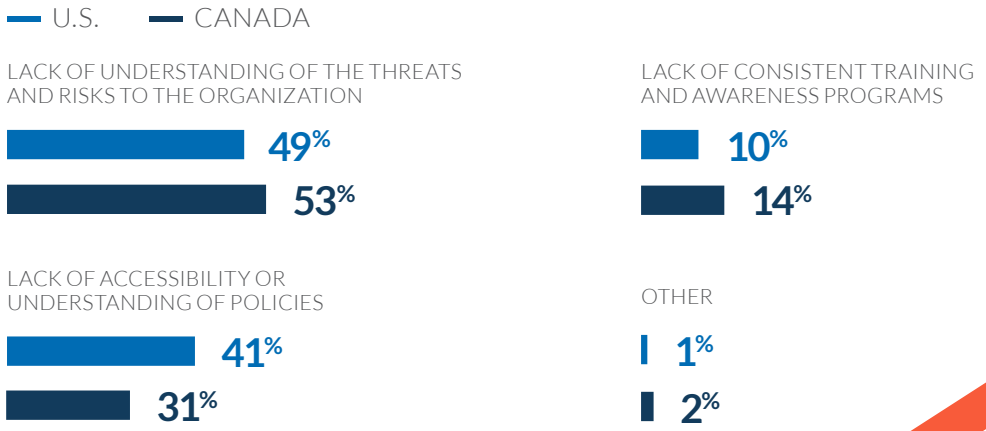
Despite Policies and Training, Employees Struggle to Put Learnings into Practice

While policies and training are an essential component of a business's information protection strategy, it is also important for employees to be aware of how critical understanding the threats of a data breach and following policies are. Many businesses realize that they can't do it alone. Across all industries surveyed, three-quarters of business leaders in the U.S. have hired a third-party security expert to evaluate security practices. This holds true with responses from the 2020 DPR as well.

Approximately half of North American business leaders (U.S. 49% and Canada 53%) indicate that the lack of understanding of the threats and risks to the organization is the biggest barrier to employees following information security policies. This is followed by lack of accessibility or understanding of policies (U.S. 41% and Canada 31%) as the next biggest barrier.

Two-thirds of Canadian and half of U.S. employees working for companies with cybersecurity policies believe required training and periodic reminders will help with employee adherence to information security policies. While half of American employees believe that leadership communication will improve adherence, only 1 in 4 Canadians agree.

Biggest Barriers to Employees Following Information Security Policies and Procedures



Approximately

50% OF

BUSINESS LEADERS

surveyed indicate that the lack of understanding of the threats and risks to the organization is the biggest barrier to employees following information security policies

RECOMMENDATIONS

As the findings of the survey have indicated, businesses must invest in data security now or face the consequences. Though the landscape is ever-changing, businesses can ensure their data is protected by staying informed on laws and regulations, understanding the kind of data they are collecting, and fostering a security-minded corporate culture.

Know the Rules: Stay Informed on Consumer Privacy and Security Laws

As the previous insights highlighted, consumers vote with their wallets, working with businesses that prioritize keeping their data private and secure. Over the last decade, data protection laws and regulations have undergone a stark evolution to not only deter the criminal but to compel organizations to act. Both factors are the impetus for businesses to take action or face eroding consumer trust as well as potentially hefty legal and financial consequences.

While some countries have federal consumer privacy and data protection legislation, the U.S. utilizes a state-by-state approach. However, recent consumer data protection laws in several states may bring the federal government closer to a tipping point. Large national and global companies will likely push for a national law because the cost of compliance and managing against 50 different privacy and data protection laws will be untenable. Therefore, keeping abreast of data protection legislation is crucial for businesses. Organizations should consider the following to stay ahead:

- **Be ready for new legislation in the U.S.**
  Three states, including California, Colorado, and Virginia, have statutes in place that govern how organizations must protect consumers' personal information and establish privacy rights for individuals. More are likely to follow.

- **Be prepared for changes in Canada as well.**
  Canada's Personal Information Protection and Electronic Documents Act, or PIPEDA, is expected to be replaced by the Consumer Privacy Protection Act. Drafts of that new legislation include monetary penalties of up to 5% of global revenue for violations. It also outlines the right of consumers to 'be forgotten' from a data perspective.

- **Think globally.**
  The statutory requirements that comprise the General Data Protection Regulation (GDPR) apply to all organizations that collect, process, or utilize personal information from individuals who live in the European Union (EU), regardless of where the business or data is located. For instance, if a company located outside of the EU provides goods or services and processes personal data or monitors the behavior of individuals in the EU they are subject to GDPR.

- **Monitor data sovereignty requirements.**
  Many nations continue to require organizations to keep certain kinds of information, including various forms of personal data, on servers located within their borders.

Know Your Data: It Pays to Be Aware

Considering the risks and financial resources as well as the reputational and operational costs associated with a data breach, being prepared is essential to minimizing the impact. Remember that a data breach can result in more extensive impacts than just ransomware payments or lost business.

So, what can businesses do to protect themselves? The first step is knowing your data. Ask yourself, what data do we have, where do we keep it, and with whom do we share it? Answering these questions is the first step in making intelligent decisions, both in creating an effective data security plan and in the investments required to implement it. Consider the following components when protecting your data:

- **Develop a comprehensive plan that covers all data.**
  Account for both electronic and paper documents in your security sweeps. All data should be destroyed on a regular cadence in alignment with statutory guidelines and best practices. The same expectations around document retention and destruction should be required of partners and contractors and should be included as a requirement for all requests for proposals and contracts.

- **Employ a data minimization strategy.**
  Ensure that you only collect, use, process, or store the information you need to carry out your business. Put a record management plan in place. Only retain what you need for only as long as you are required to keep it.

- **Evaluate your IT infrastructure and practices.**
  Access the right IT expertise. Few IT organizations have the expertise in-house required to monitor today's fast-evolving threat landscape or the tools and technology required to combat an ever-growing array of cyber threats. For many organizations, subscription-based security and data protection services are a proven solution for resource-constrained IT teams.

- **Embrace the cloud.**
  Reputable cloud providers have the most progressive security solutions in place and deploy security resources that dwarf those of even the most advanced companies. With most data breaches occurring in on-premises data centers, networks, or systems, make sure to back up everything and do it frequently. Today's disaster recovery and backup solutions take advantage of the cloud's inherent elasticity and make frequent snapshots of the entire dataset possible at intervals of the customer's choosing.

- **Encrypt important data on-premises, in the cloud, and in transit.**
  Using encryption that aligns with current industry standards will often shield an organization from civil litigation even if consumers' data is compromised.

- **Invest in an endpoint detection and response (EDR) technology.**
  Investing in EDR technology safeguards the edge of the network, often its most vulnerable point. Most importantly, deploy a network monitoring solution that alerts IT of suspicious activity in real-time and take action. You cannot combat what you cannot see.

Prepare to Act: Policies Are Not Enough; Protecting Data Is a Team Sport

A business's best line of defense starts inside. Equipping employees with the proper tools and knowledge will empower them to become ambassadors for information security—encouraging others to do the same. Companies should also ensure they know what vendors are doing to keep their information safe. To create a strong line of defense to prevent a data breach, businesses should:

Create a security-minded corporate culture for data protection best practices.

Data is the lifeblood of any organization and protecting it is a team sport. It's important that employees understand the full picture impact of a breach. Not only does a breach impact day-to-day business, but it could impact their job security.

Institute policies accompanied by role-based training.

Businesses should implement policies to address the information security of the enterprise, the privacy of consumers' data, regulatory security guidelines (such as those for HIPAA in healthcare and the Gramm-Leach-Bliley Act in financial services), and physical security for data in all forms—including electronic and printed documents. But, for a policy to be effective, businesses should provide training programs to help employees put the information into practice to ensure understanding and adherence.

Evaluate your data protection policies.

Businesses should institute policies to ensure employees understand the expectation around document handling and retention. Policies, such as a clean desk, shred-it-all, and remote work will take the guesswork out of secure document handling and reduce the risk of human error. The policy must clearly state the expectations and the steps that will be taken when violations occur.

Train employees to be a viable front line of defense.

Policies are only just the beginning. Employees should be trained to ensure they understand and can implement the expectations outlined in the policy. Businesses can employ a variety of training initiatives such as phishing simulations to encourage employees to be vigilant and promote adherence. Incentives can also be used to reward employees that report security dangers. The enthusiasm that results pushes data protection programs and initiatives forward.

Address insider threats.

Consider implementing two-factor authentication for all users when accessing critical systems and applications. Also consider a zero-trust approach to network access requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and validated for security configuration prior to being granted access to applications and data.

Employ an incident response plan.

Demonstrate competence in your response to any data breach by preparing yourself with an incident response plan. Make sure that you have a mitigation and communications plan that will enable you to move quickly. Consumers rapidly lose trust in brands and organizations that do not alert them of a security breach involving their personal data in a timely manner. Provide customers with transparency about what happened and how the company is taking steps to prevent a data breach from happening in the future.

Invest in cyber insurance and expert help.

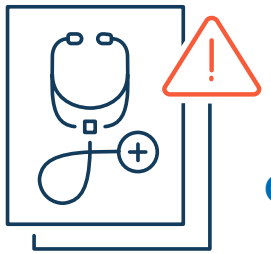
These services can help cover the cost of legal services and advice as well as crisis management services. Additionally, they can inform and prepare a businesses' response to a data breach including notification of affected parties (business customers or individuals whose data was accessed or acquired during the breach).

INDUSTRY SPECIFIC INSIGHTS

The 2021 DPR includes an in-depth review of industry-specific practices throughout the healthcare, finance, professional services, insurance, and real estate industries. In general, all businesses surveyed agree that information security is important to their company. Yet each faces a unique set of realities when it comes to their data protection preparedness.

The Best Medicine: Healthcare Industry Preparedness Combats Cyber Attacks

In 2020, there was a 73% increase in the number of confirmed data breaches in the healthcare industry.[1] These incidents exposed 12 billion pieces of protected health information (PHI).[1] Within this context, healthcare organizations would be well advised to continue their vigilance.



56% OF **HEALTHCARE ORGANIZATIONS**

Surveyed Have Ever Experienced a Data Breach

29% OF **HEALTHCARE ORGANIZATIONS**

Surveyed State a Data Breach Occurred in the Past 12 Months

Healthcare Organizations Understand that it Pays to Be Prepared

75% State Information Security Is Very Important to Their Company

62% Believe a Data Breach Would Be Costly*

54% Feel a Data Breach Would Have a Major Impact on Their Reputation

61% Have Hired a Third-Party Security Expert to Evaluate Security Practices

*In terms of money and time taken to rectify the situation.

Healthcare Organizations Are Better Equipped than Companies in Other Industries

More than any other industry, 65% of healthcare organizations say that their organization has access to the appropriate information security tools and resources. They are significantly more likely than any other industry to have an incident response plan leading to faster incident recovery times than other industries.

Policies and Protection Strategies

- **64%** Employ Information Security Policies
- **48%** Have Regular Infrastructure Auditing
- **27%** Have a Paper Shredding Service to Protect Against Data Breaches
- **85%** Have a Cyber Insurance Policy
- **33%** Perform Vulnerability Assessments

Response Plan

- **58%** Have an Incident Response Plan
- **35%** Took a Few Weeks to Resolve the Most Recent Data Breach

Taking Stock: Finance Industry Excels in Employing Information Security Policies

From Social Security numbers and credit reports to monthly income receipts and more, customers must submit copious amounts of personally identifiable information (PII) when working with financial organizations. If any of this information falls into the wrong hands, it could put customers at serious risk for identity theft or fraud. While financial organizations are not immune to data breaches, they are investing in resources to protect against future breaches.

52% OF **FINANCIAL ORGANIZATIONS**

Surveyed Have Ever Experienced a Data Breach

42% OF **FINANCIAL ORGANIZATIONS**

Surveyed State a Data Breach Occurred in the Past 12 Months

Finance Organizations Understand that it Pays to Be Prepared

40% State Information Security Is Very Important to Their Company

47% Believe a Data Breach Would Be Costly*

49% Feel a Data Breach Would Have a Major Impact on Their Reputation

80% Have Hired a Third-Party Security Expert to Evaluate Security Practices

*In terms of money and time taken to rectify the situation.

Financial Organizations Feel They Are Equipped

The financial industry is confident in the measures they have in place to create a security-minded corporate culture, as 62% believe they have access to the appropriate tools and support. And, while they excel in policy implementation, there is room for improvement in protecting against physical data breaches with a shredding service.

Policies and Protection Strategies

- **72%** Employ Information Security Policies
- **89%** Have a Cyber Insurance Policy
- **43%** Have Regular Infrastructure Auditing
- **38%** Perform Vulnerability Assessments
- **13%** Have a Paper Shredding Service to Protect Against Data Breaches

Response Plan

- **40%** Have an Incident Response Plan
- **44%** Took a Few Weeks to Resolve the Most Recent Data Breach

Adding It All Up: Professional Services Rethinks Sharing Data with Service Providers

As nefarious characters become more sophisticated in their approach, they become increasingly harder to spot. Nearly half (41%) of professional services surveyed are more likely to say that sharing data with third parties is seen as a significant information security risk. With this in mind, professional services must create a security-minded corporate culture to strengthen their first line of defense against data breaches—their employees and service providers.

51% OF **PROFESSIONAL SERVICES**

Surveyed Have Ever Experienced a Data Breach

40% OF **PROFESSIONAL SERVICES**

Surveyed State a Data Breach Occurred in the Past 12 Months

Professional Services Understands that it Pays to Be Prepared

55%
State Information Security Is Very Important to Their Company

40%
Believe a Data Breach Would Be Costly*

35%
Feel a Data Breach Would Have a Major Impact on Their Reputation

69%
Have Hired a Third-Party Security Expert to Evaluate Security Practices

*In terms of money and time taken to rectify the situation.

Professional Services Are Most Concerned about Documents Left Out in the Open

Professional services are most concerned about employees leaving confidential documents on their desk (71%), yet only a quarter have paper shredding services. With physical document exposure leaving businesses at risk, these organizations would be well-advised to invest in policy and protection strategies to mitigate the possibility of a data breach.

Policies and Protection Strategies

- **56%** Employ Information Security Policies
- **44%** Have Regular Infrastructure Auditing
- **25%** Have a Paper Shredding Service to Protect Against Data Breaches
- **69%** Have a Cyber Insurance Policy
- **36%** Perform Vulnerability Assessments

Response Plan

- **38%** Have an Incident Response Plan
- **30%** Took about a Month to Resolve the Most Recent Data Breach

Protecting the Protectors: Insurance Industry Turns to Security Experts for Guidance

Insurance organizations are known to store large amounts of personally identifiable information (PII) about their policyholders, making them a target for cybercrime. And, compared to the other industries surveyed, insurance comes out on top of those who have experienced a data breach.

75% OF **INSURANCE ORGANIZATIONS**

Surveyed Have Ever Experienced a Data Breach

65% OF **INSURANCE ORGANIZATIONS**

Surveyed State a Data Breach Occurred in the Past 12 Months

Insurance Organizations Understand that it Pays to Be Prepared

44% State Information Security Is Very Important to Their Company

39% Believe a Data Breach Would Be Costly*

43% Feel a Data Breach Would Have a Major Impact on Their Reputation

84% Have Hired a Third-Party Security Expert to Evaluate Security Practices

*In terms of money and time taken to rectify the situation.

Insurance Organizations Are Most Concerned about Documents Left Out in the Open

Insurance companies who have experienced a breach understand the importance of destroying sensitive materials when no longer needed to improve business processes and protect sensitive information from unauthorized access. Yet, the majority (85%) of insurance companies surveyed are concerned about employees leaving confidential materials out on their desks. Insurance organizations need to relook at their data protection strategy against physical data breaches, as most reported not having a paper shredding service.

Policies and Protection Strategies

- **50%** Employ Information Security Policies
- **25%** Have Regular Infrastructure Auditing
- **6%** Have a Paper Shredding Service to Protect Against Data Breaches
- **90%** Have a Cyber Insurance Policy
- **13%** Perform Vulnerability Assessments

Response Plan

- **25%** Have an Incident Response Plan
- **49%** Took About a Month to Resolve the Most Recent Data Breach

Location, Location, Location: Real Estate Industry Lacks in Incident Response Planning

Reputation is essential to client retention in the real estate industry, and with rising consumer expectations around information security, they understand the importance of keeping their information secure.

69% OF
REAL ESTATE ORGANIZATIONS
Surveyed Have Ever Experienced a Data Breach

58% OF
REAL ESTATE ORGANIZATIONS
Surveyed State a Data Breach Occurred in the Past 12 Months

Real Estate Organizations Understand that it Pays to Be Prepared

57%
State Information Security Is Very Important to Their Company

46%
Believe a Data Breach Would Be Costly*

42%
Feel a Data Breach Would Have a Major Impact on Their Reputation

77%
Have Hired a Third-Party Security Expert to Evaluate Security Practices

*In terms of money and time taken to rectify the situation.

Real Estate Organizations Feel They Are Equipped

The real estate industry has the measures in place to create a security-minded corporate culture, as 56% believe they have access to the appropriate tools and support. While they excel in employing policies, there is room for improvement in incident response planning.

Policies and Protection Strategies

- **64%** Employ Information Security Policies
- **88%** Have a Cyber Insurance Policy
- **33%** Have Regular Infrastructure Auditing
- **19%** Perform Vulnerability Assessments
- **15%** Have a Paper Shredding Service to Protect Against Data Breaches

Response Plan

- **29%** Have an Incident Response Plan
- **47%** Took a Few Weeks to Resolve the Most Recent Data Breach

Conclusion: Invest Now or Pay Later

The 2021 Shred-it Data Protection Report confirms that North American businesses, large and small, can no longer consider data protection and security an optional investment. Yes, today's data protection landscape can be overwhelming, but it is not impossible to manage. By educating themselves, ensuring they are equipped with the right services and expertise, and planning—before the breach—every company can balance risk and reward when protecting the health and well-being of their trusted relationships, bottom line, and brand.

> **In fact, organizations that go beyond simple regulatory compliance can build trust with customers and stand out from competitors.**

The 2021 DPR outlines key insights and recommendations to help guide your path forward:

- **Understand the rules.**
  Currently, three states have laws in place to protect consumers' information and have established individual privacy rights. Canada is looking to enact new legislation, PIPEDA, to replace CPPA. As the regulatory requirements continue to evolve, it is essential that businesses stay up-to-date.

- **Know your data.**
  An ounce of prevention is worth a pound of cure. Take inventory of the types of data you collect, how you store it, and with whom you share it. These details are key to implementing an effective data security plan.

- **Prepare to act.**
  Policies are not enough. Protecting data is a team sport. Equip employees with the right knowledge and tools, and provide frequent reminders and incentives to keep data security top of mind. It pays to have mitigation strategies and a response plan in place to protect your brand and your bottom line.

The Need to Protect Data Has Never Been More Important

Keeping up with regulations and consumer expectations is a lot to juggle, but you don't have to do it alone. To ensure you have visibility to the rapidly changing threat landscape and the technologies available to combat it, partner with an expert service provider to help you bridge any gaps.

Choose the information security partner that can help you meet the growing information security challenges facing your organization. With industry-leading information security services, Stericycle's Shred-it document destruction service can protect the health and well-being of your business, safeguarding your data and your reputation.

Security Expertise

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

Service Reliability

Whether you're a large-scale national enterprise or a small business, 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, we are committed to your protection.

Learn more about information security and how we can help protect your organization at www.shredit.com or call 800-697-4733.

We protect what matters.

About the Survey

The 2021 DPR survey respondents included consumers as well as executives (titles: owner, executive, C-level, Vice President, IT Director or above, defined by the number of employees in the organization) across North America (U.S. and Canada). These businesses represented the healthcare, finance, professional services (engineering, accounting, and research), insurance, and real estate industries.

Small and medium sized businesses were defined as having 20-499 employees and large businesses were defined as having 500 or more employees. Quotas were set to be nationally representative based on gender, age, and geographic region for the U.S. and Canada separately. In addition, only employees and owners of businesses having familiarity with the company's information security policies and procedures were surveyed.

400
CONSUMERS

125
C-LEVEL EXECUTIVES

139
SMALL AND MEDIUM BUSINESS OWNERS

SOURCES

1. Verizon, Data Breach Investigation Report, 2021.
2. Ponemon Institute, IBM Security Cost of Data Breach Report, 2021.
3. Ponemon Institute, IBM Security Cost of Data Breach Report, 2018.
4. The Drum, The current state of US state data privacy laws, April 26, 2021.
5. Risk Based Security, Year End Report, 2020.
6. Zendesk, Customer Experience Trends Report, 2020.

Shred-it®
A Stericycle® Solution