Shred-it®

A Stericycle® Solution

DATA PROTECTION REPORT 2022

The Vital Importance of Data Protection for Small Businesses

We protect what matters.

Table of Contents

Key Takeaways from the Report Reveal:

- Small Businesses Are Leaving Physical Data Vulnerable to Potential Breaches
- Education Is Key in Data Protection Efforts
- Third-Party Partners Can Play a Key Role in Developing a Compliance Strategy

Foreword

The world we live and work in today is drastically different than just a few years ago. A global pandemic has altered the way we work and collaborate within our organizations and with customers, putting enormous stress on organizations' information security systems. While data breaches are at an all-time high,[1] physical breaches—including document theft—accounted for 43% of breached assets in 2021.[2]

Ineffective data protection strategies and bandage security solutions will not hold up against today's data breaches. Business leaders—especially at small businesses—must understand the potential impact of insufficient data protection, not only to protect their bottom line but also to safeguard their reputation with employees and customers. Leaders need to prioritize both digital and physical information security efforts and remain educated about changes in data protection legislation to ensure compliance.

This can be especially difficult for small businesses, which often have smaller budgets and limited resources.

In support of our mission to help organizations protect what matters, Shred-it, a Stericycle solution, has drawn on our expertise as a world leader in secure information destruction services to field an in-depth survey of small business leaders across North America to produce our 12th annual Data Protection Report (DPR). We are committed to protecting the health and well-being of our clients' businesses, trusted relationships, and brand reputation. The 2022 DPR was specifically developed to offer small businesses in the United States and Canada key insights and actionable steps to help protect their organizations.

To our 2022 survey contributors, thank you. Your perspectives and insights will be a powerful resource for small businesses as they navigate the complexities of information security. To our readers, Stericycle, through our Shred-it secure information destruction solution, is here as a trusted partner. Our team is ready to help your organization navigate the complexities of the evolving 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

Executive Summary

The last few years have been rife with data protection risks. A global pandemic accelerated a shift to remote work environments for most organizations. The "Great Reshuffle," a time of strong labor demand and low unemployment, led to high employee turnover[3] across North America. With a swath of new employees working in a hybrid and decentralized work environment, there has never been a more important time, especially for small businesses, to prioritize data protection.

According to Identity Theft Resource Center's 2021 Annual Data Breach Report, last year had the highest number[1] of reported data breaches at 1,862, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017. In addition, according to IBM's Cost of a Data Breach Report, the average cost of a data breach[4] also rose in 2021 to $4.24 million, a 10% rise from the average cost in 2019. Even smaller organizations with less than 500 employees saw a 26.8% increase in the average cost of data breaches.[4]

The financial impact of a data breach could cripple a small business as they face the potential for regulatory actions and fines, legal fees, and the loss of customers, as well as long-term impacts such as damage to brand reputation and depressed recruitment. Given these ramifications, small business owners need to understand how data breaches occur and how to best prepare themselves. Data breaches fall into two primary categories: physical and digital. Physical security risks include the theft of items such as proprietary business records, employee files, tax filings, customer information, and medical records. Digital security risks are comprised of unauthorized access, system or human error, or a deliberate attack on a system or network. Developing a data protection strategy that prioritizes both digital and physical security risks is crucial in combatting data breaches.

Physical Security Risks

PAPER DOCUMENTS | LAPTOP COMPUTERS | EXTERNAL HARD DRIVES

Digital Security Risks

MALWARE | RANSOMWARE | PHISHING

Average Cost of a Data Breach For Small Businesses[4]

(Measured in U.S. $ millions)

26.8%

INCREASE

from 2020 to 2021

We protect what matters.

Key Insights

Based on in-depth 2022 survey data and analysis of the perspectives of U.S. and Canadian small business leaders (SBLs), Shred-it's 2022 DPR reveals crucial insights on information security concerns and challenges today. It also reveals SBLs' perceptions of the current regulatory landscape and top barriers with compliance, as well as assesses the demand for assistance from external partners. This year's report delivers actionable steps for SBLs to take to help navigate a complex and ever-changing data protection regulatory environment. Key insights include:

Small Businesses Are Leaving Physical Data Vulnerable to Potential Breaches

Even though the vast majority (91%) believe that physical and digital data protection are equally important, many SBLs (53%) assert that digital risks are the greatest data protection risk to their business today. And only 27% of SBLs say they collect and destroy sensitive materials when no longer needed.

Education Is Key in Data Protection Efforts

Only 58% of SBLs say their companies require all employees to undergo mandatory information security training. Even with that training, SBLs fear that their workforce still does not understand data protection best practices (67%) or how to navigate a potential data breach (66%).

Small Business Leaders Need Support to Navigate a Changing Regulatory Landscape

Nearly eight out of 10 SBLs believe that their businesses are disproportionately affected by regulations compared to large businesses, which often have more resources for support. Seventy-five percent of SBLs are worried that future changes will only make regulations more difficult, complex, and burdensome, and 60% fear their businesses won't be able to keep up with new privacy mandates or reporting requirements.

Survey Respondents Comprised Of:

Small Business Leaders
(15-100 Employees)
in the U.S. and Canada

ACROSS A VARIETY OF SECTORS, INCLUDING:

Healthcare

Finance

Professional Services

Insurance

Real Estate

SBLs' Perspectives on the Information Security Landscape

More than **90%** OF **SBLs** believe that physical and digital risks are equally important

However, only **27%** OF **SBLs** state that they collect and destroy sensitive materials when no longer needed (e.g., printed materials, computers, hard drives)

Even with training, **67%** OF **SBLs** fear that their workforce does not understand data security best practices

Nearly **8** OUT OF **10** **SBLs** believe that their businesses are disproportionately affected by regulations compared to large businesses

CURRENT DATA PROTECTION PRACTICES

Small Businesses Are Spending More on Digital Data and Information Protection Measures

But Are They Still Leaving Their Physical Data Vulnerable to Potential Breaches?

Small Businesses Are Spending More on Digital Data Protection Than Ever Before

According to the Identity Theft Resource Center's 2021 Data Breach Report,[1] the number of reported data breaches jumped 68% last year to the highest total ever. Unsurprisingly, the majority (90%) of SBLs surveyed in the DPR believe that data protection has never been more important than it is today and reported that it is a top priority for their company.

In fact, two-thirds of SBLs reported having spent more budget on data and information protection measures this year than ever before. With those dollars, most SBLs (85%) believe they are deploying the "best tools" to help keep organizational and customer data safe and protected. But is it enough?

When asked about the reason for the increases in their company's data and information protection budget, SBLs said:

> **"With today's evolving technology, we want to be able to keep up. And that includes updating and upgrading our company's data protection program. And with better things comes the increase in price to acquire it."**

> **"Our clients are increasingly requiring more stringent data protection policies."**

2 OUT OF **3** **SBLs**

report having spent more budget on data and information protection measures this year than ever before

Small Businesses Are Leaving Physical Data Vulnerable to Potential Breaches

Even though the vast majority (91%) believe that physical and digital data protection are equally important, many SBLs (53%) assert that digital risks are the greatest data protection risk to their business today. This may have driven SBLs to prioritize more digital security measures to protect their company's most sensitive information, like deploying anti-virus programs (40%) or frequent software updates (28%).

However, as SBLs prioritize digital risks, their organizations are left exposed and more vulnerable to physical risks. Only 27% of SBLs indicate that they collect and destroy sensitive materials when no longer needed (e.g., printed materials, computers, hard drives). This may suggest that SBLs need to prioritize protecting their company's sensitive physical materials, in addition to putting more stringent digital safeguards in place.

Actions Taken by SBLs to Keep Sensitive Data and Information Safe

PHYSICAL

27% Collect and destroy sensitive materials when no longer needed (e.g., printed materials, computers, hard drives)

DIGITAL

40% Deploy anti-virus programs

28% Provide frequent software updates

25% Implement two-factor authentication

24% Deploy automated security defenses to detect, investigate, and remediate data security threats

BOTH PHYSICAL AND DIGITAL

28% Limit sharing of data with third parties

27% Provide data and information protection awareness training for employees

23% Conduct vulnerability assessments

23% Implement and enforce record retention and destruction policies

20% Establish incident response plans

THE EMPLOYEE EDUCATION GAP

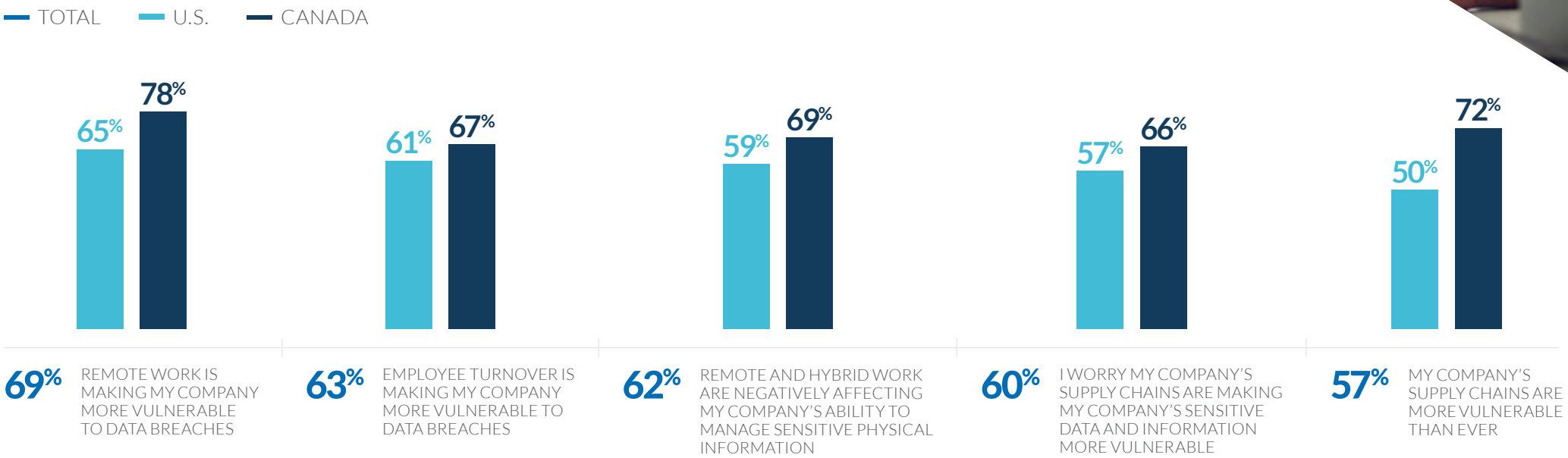
SBLs Are Facing Challenges in Protecting Their Company's Sensitive Data and Information

Although They Acknowledge Education Is Key, It Is Still Lacking

SBLs Face Challenges in Protecting Their Company's Sensitive Data and Information

Despite their best efforts to prioritize and invest in data protection, the vast majority (90%) of SBLs admit it has never been harder to keep their company's sensitive data and information safe, and at least two-thirds feel anxious or fearful about the safety of their company's data. While only 23% of SBLs say they have experienced a data breach, 66% fear their business is vulnerable to data breaches. Remote work (69%), employee turnover (63%), and supply chain vulnerabilities (60%) are all driving factors of small business owners' data protection challenges and concerns today.

Top Driving Factors of Data and Information Protection Challenges



69% REMOTE WORK IS MAKING MY COMPANY MORE VULNERABLE TO DATA BREACHES

63% EMPLOYEE TURNOVER IS MAKING MY COMPANY MORE VULNERABLE TO DATA BREACHES

62% REMOTE AND HYBRID WORK ARE NEGATIVELY AFFECTING MY COMPANY'S ABILITY TO MANAGE SENSITIVE PHYSICAL INFORMATION

60% I WORRY MY COMPANY'S SUPPLY CHAINS ARE MAKING MY COMPANY'S SENSITIVE DATA AND INFORMATION MORE VULNERABLE

57% MY COMPANY'S SUPPLY CHAINS ARE MORE VULNERABLE THAN EVER

Employee Error Is a Key Vulnerability

While only 1 in 4 say they have experienced a data breach in the past, SBLs believe employee error is a key vulnerability. In fact, according to Verizon's 2022 Data Breach Investigation Report,[5] 82% of breaches this year involved the human element, including stolen credentials, phishing, or misuse. Furthermore, the report also found that despite the pandemic and less travel, assets remained vulnerable to being lost or stolen. This includes portable employee devices—such as desktops, laptops, and mobile phones—and printed documents.

When asked about their company's data and information protection challenges, one SBL said:

> **"Primarily education. A lot of employees don't know the variety of ways in which scammers can access your data. We often experience email breaches because people don't understand what to look for to protect themselves."**

Additionally, SBLs fear that—even with their best efforts to train employees—their workforce still does not understand data security best practices (67%) or how to navigate a potential data breach (66%). High employee turnover is one of the biggest challenges when training employees and, according to a survey from Principal Finance Group, the majority of small businesses reported[6] experiencing high turnover due to COVID-19. Besides, half of SBLs agree they don't know what actions to take if a data breach were to occur. In their own words, small business leaders cite a lack of education as an ongoing data protection challenge.

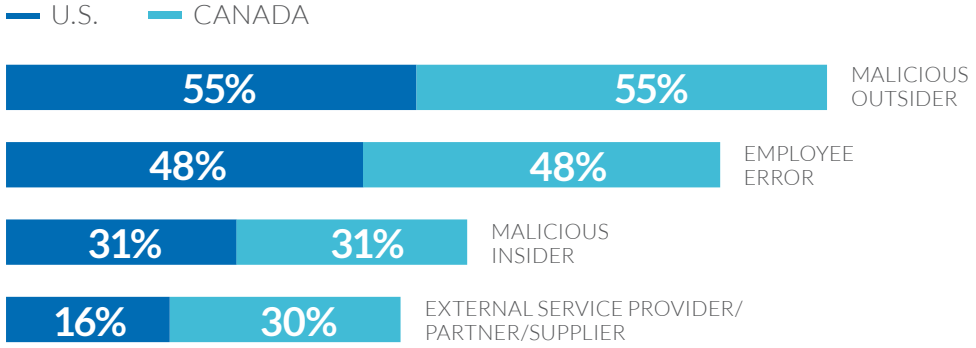
67% OF SBLs

fear that their employees don't know best practices to **prevent** a data breach

66% OF SBLs

fear that their employees don't know **what actions to take** if a data breach occurs

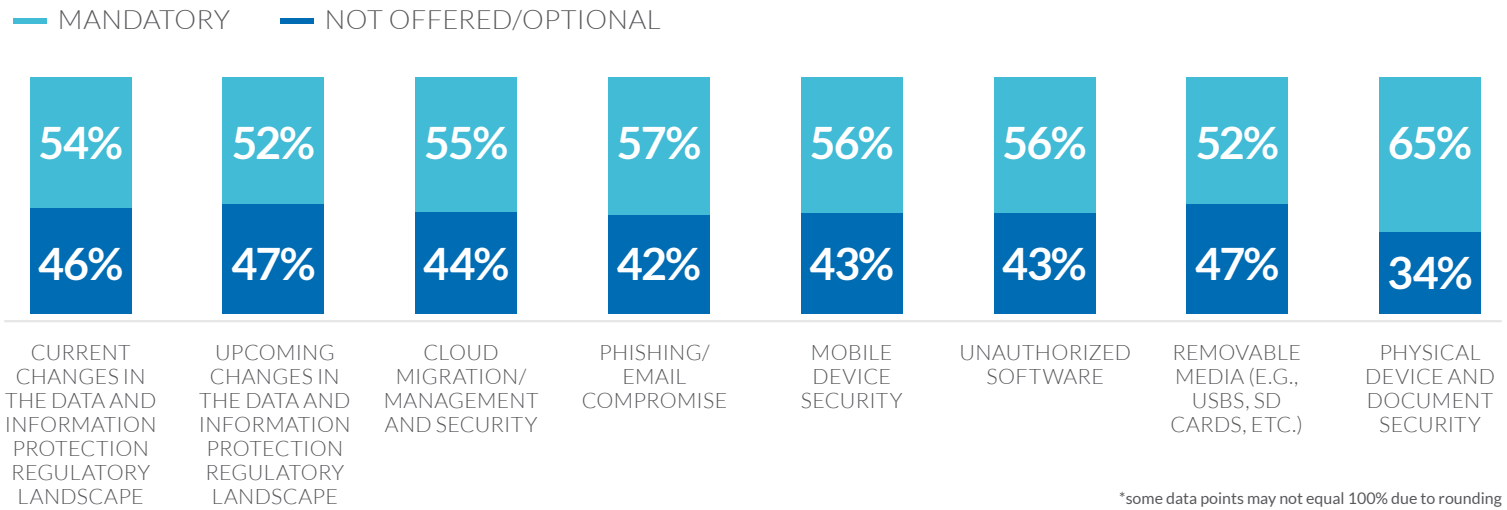
Sources of Data Breaches According to SBLs



Education Is Key in Data Protection Efforts But Lacking

While the importance of data protection training for employees is not questioned, only 58% of SBLs say their companies require all employees to undergo mandatory data and information protection training. The majority of SBLs (65%) worry that what they offer is still not enough. When asked about trainings that are provided to their employees, too many critical data and information protection trainings are only being offered as optional, or not at all.

SBL Data and Information Protection Training Practices



*some data points may not equal 100% due to rounding

A majority of SBLs (83%) desire a way to simplify their security training approach to properly educate their employees, and many (US: 50% and Canada: 60%) lack a reliable source—be it internal or external—to consistently maintain their data and information protection policies and trainings.

For SBLs, it may seem harder than ever to protect sensitive company data and information. But their current training regimens and level of employee knowledge is not keeping pace, and SBLs know it. These are key weaknesses that, if properly addressed, could help relieve some SBLs' concerns about data protection risks.

8 IN 10

SBLs

wish they had a way to simplify their security awareness training

More than

50% OF

SBLs

lack a reliable source—be it internal or external—to consistently maintain their data and information protection policies and trainings

THE REGULATORY LANDSCAPE AND FUTURE OUTLOOK

Small Businesses See the Value in Data Protection But Struggle to Understand and Comply

Third-Party Partners Can Play a Key Role in Developing a Compliance Strategy

Small Businesses Struggle with Regulatory Compliance

While SBLs see the value of data and information protection regulations—calling them necessary (46%) and beneficial (38%), more than half also say they struggle with compliance due to regulatory changes and lack of key resources.

Large businesses often have more resources in the form of staff, tools, and funding to meet and even get ahead of changing data and information protection regulation. Small businesses, who may not have a dedicated compliance or IT team or budget, may have a harder time navigating changing regulations. In fact, 8 in 10 SBLs think their businesses are being disproportionately affected by regulations compared to large businesses.

When asked about today's data and information protection environment, one SBL said:

> **"Small businesses like ours don't have the resources to face today's data and information protection regulatory environment."**

SBLs' Concerns on Current Data and Information Regulations

58% cannot keep track of changing data and information protection regulations

55% do not have adequate resources or support to navigate today's data and information protection regulations

25% do not understand the various types of data and information protection laws and the ways businesses are subject to comply

Trusted Partners Can Help Relieve the Stress of Potential Regulatory Changes

The majority of SBLs (75%) are worried that the road ahead will only become more difficult, complex, and burdensome for their businesses. Sixty-five percent of SBLs feel overwhelmed by the thought of future data and information protection regulation changes, and 60% fear their businesses won't be able to keep up with new privacy mandates or reporting requirements.

Collaborating with a trusted third-party security partner can help small businesses comply with the shifting regulatory landscape. About half of SBLs say they are currently working with a partner to help manage digital (55%) and physical (45%) data.

Traits SBLs Are Looking for in a Data and Information Security Partner

95%
are looking for a partner that can help them comply with data and information protection regulations

94%
are looking for a partner that understands the changing data and information protection regulations

93%
are looking for a partner that is knowledgeable of their legal obligations when it comes to data and information protection

SBLs are most in need of support when managing their sensitive digital (52%) and physical (32%) data and information, strengthening current protection policies (31%), and ensuring information in remote and hybrid working environments is secure (28%).

SBLs see the value in data protection regulations but find the shifting regulatory landscape challenging to navigate, understand, and comply with. Partnering with the right trusted third party for data protection, management, and compliance can help SBLs navigate the difficult environment and feel more confident in their organization's ability to protect their company's sensitive data and information.

52% OF SBLs
need support in managing their sensitive **digital** data and information

32% OF SBLs
need support in managing their sensitive **physical** data and information

31% OF SBLs
need support in strengthening current protection policies

Recommendations: Secure Your Data and Stay Informed

The last few years have created more security challenges for small businesses than ever before. SBLs should prioritize their data security efforts in order to avoid a potential data breach. The following are steps that a small business can take to help keep its information and data safe.

Invest in both physical and digital security measures.

If protecting sensitive data and information is a top priority for SBLs today, then they need to prioritize protecting their company's sensitive physical information, in addition to putting digital safeguards in place. Physical information continues to be at risk of a breach, especially as businesses adopt hybrid work models where sensitive paper documents may be regularly carried from offices to homes and back. To help keep organizations fully protected from data breaches, small business leaders should consider the importance of physical data protection.

SBLs should also consider implementing and enforcing record retention and destruction policies in both office and remote work settings to help improve physical data security protocols. For example, a clean desk policy helps ensure that all sensitive physical documents are either stored or destroyed each time an employee leaves their desk, which helps prevent information theft. Businesses should also collect all documents that are no longer needed in a secure, locked container to be shredded.

Provide mandatory data security education.

Employees can be an organization's first and best defense against a data breach. SBLs know that their current training regimens and level of employee knowledge are not up to par and likely worsen due to high employee turnover. These are key weaknesses that, if properly addressed, could help improve small business owners' data security.

To equip their employees with the skills they need to recognize and respond to data breach threats, small businesses should provide regular and mandatory data security training for all employees. New hires should also undergo in-depth security training as part of the onboarding process. Effective data security training will help employees identify both physical and digital data security risk factors and explain how to try to prevent a data breach in an approachable and engaging way.

Find a trusted third-party partner to support your data protection and education efforts.

SBLs often must fulfill a wide range of responsibilities, from managing their organization's finances, to marketing, to HR. With all these obligations, most SBLs lack the time and skills to lead their organization's data security protocols alone. Many small businesses see the value in data protection regulations but find the shifting regulatory landscape complex, burdensome, and costly.

Partnering with the right trusted third party for data protection, management, and compliance can help SBLs navigate the difficult environment and feel more confident in their organization's ability to protect their company's sensitive data and information. Trusted third-party partners provide SBLs with effective data protection tools, services, and employee training programs that meet their organizations needs.

CONCLUSION

Small business leaders know that data security is a necessary foundational element in building and retaining strong relationships with their customers, employees, and partners. However, with less budget and fewer resources than larger organizations, small businesses may struggle to practice comprehensive data security, offer regular, effective employee training, and understand the shifting data protection regulatory landscape.

To help protect their organizations from data breaches, SBLs should enlist the support of trusted partners to help them understand and navigate the complexities of data protection regulations and provide necessary employee training. The right third-party partner will help guide SBLs through the evolving regulatory landscape and empower them to become more knowledgeable. A third-party partner can also provide a comprehensive employee training strategy to enable employees to recognize and respond to data security threats. Taking these steps toward better data protection can benefit a small business' bottom line and brand reputation today and in the future.

The Need to Protect Data Has Never Been More Important

Keeping up with regulations and consumer expectations is a lot to juggle, but small businesses don't have to do it alone. To help ensure you have visibility to the rapidly changing threat landscape, 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 help you protect the health and well-being of your business, by taking steps to safeguard 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 helps ensure that your confidential information remains confidential.

Service Reliability

Whether you're a small business or large-scale national enterprise, 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.

Visit Shredit.com to learn more about information security and how Shred-it can help protect your organization.

We protect what matters.

Survey Methodology

This research was conducted through a 15-minute online survey to uncover small business leaders' information security concerns and challenges with data protection today. This report also investigates perceptions of today's data protection regulatory landscape and top barriers with compliance, the future outlook, and demand for external assistance from partners. The survey utilized a variety of question types, including multiple choice, rating scale, and open ended.

The audiences of focus for this research included small business leaders (e.g., business owners, executives, C-levels, VPs, Director+ levels or equivalent) who work at or own companies with 15 to 100 employees in the U.S. and Canada across a variety of sectors (e.g., healthcare, finance, professional services, insurance, real estate, etc.).

350
U.S.

160
CANADA

510
TOTAL RESPONDENTS

SOURCES

1. Identity Theft Resource Center, Annual Data Breach Report, 2021.
2. Verizon, Data Breach Investigation Report, 2021.
3. Business Insider, American Turnover Insights, 2022.
4. IBM, Cost of a Data Breach Report, 2021.
5. Verizon, Data Breach Investigation Report, 2022.
6. Principal Financial Group, Principal Business Owner Insights, 2021.

Shred-it®
A Stericycle® Solution