Shred-it®
A Stericycle® Solution

DATA PROTECTION REPORT 2023

Vulnerable Small Businesses Risk Losing More Than Just Money

We protect what matters.℠

Table of Contents

Foreword

Following years of stress from the global pandemic, small businesses and consumers continue to face financial pressures due to inflation and rising prices. Additionally, organizations are dealing with rising costs and lingering supply chain issues. Running a business requires leaders to make difficult decisions regarding their budgets and priorities. Properly addressing data protection should be an essential part of those strategic decisions.

Historically, data breaches have increased during periods of economic uncertainty. For example, during the 2009 recession, the FBI reported a 22% increase in the number of online fraud complaints compared to 2008[1]. A volatile economy only heightens risks, making an already difficult battle more demanding. At the same time, economic struggles can also have a negative impact on an organization's response to this battle, creating an alarming confluence of factors. This can be especially difficult for small businesses, which often have smaller budgets and limited resources.

This year, the number of data breaches remains in line with the all-time high set in 2021[2], and consumers are not oblivious to the stark realities of data security risk. Moreover, the threat of data theft is driving consumers to change the ways they interact with companies, if at all. Many consumers have already been victims of data breaches, and almost all are concerned about having their personal information compromised in the future. According to a Ping Identity consumer report, 81% of consumers would stop engaging with a brand online following a data breach, including 25% who would stop interacting with the brand in any capacity[3].

Ineffective data protection strategies and "bandage" security solutions will not hold up against today's advanced threat actors. 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.

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—as well as consumers concerned about data security—across North America to produce our 13th annual Data Protection Report (DPR). In addition to small business leaders, we felt it was important to better understand the unique perspectives of consumers this year. We are committed to protecting the health and well-being of our clients' businesses, trusted relationships, and brand reputations. The 2023 DPR was developed to offer small businesses key insights and actionable steps to help protect their organizations.

We thank all of our 2023 survey contributors. Their insights and points of view are a powerful resource, helping small businesses as they manage the challenges of information security. Additionally, Stericycle, through our Shred-it® secure information destruction solution, is here as a trusted partner for any size organization. Our team can help your business 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

Key Takeaways from the Report Reveal:

- Vulnerable Small Businesses May Risk Losing Customers Due to Potential Breaches
- Training and Education Can Help Mitigate Potential Risks
- An Effective Compliance Strategy Relies on a Strong Third-Party Partnership

Executive Summary

Small businesses continue to face new challenges in their efforts to protect sensitive data and information. Many employees have left their jobs in search of roles with higher salaries, more flexibility, and the ability to continue working remotely post-pandemic. In addition to this "Great Reshuffle", the "work-from-anywhere" workplace and increased adoption of cloud-based storage systems leaves more organizations vulnerable to potential data breaches.

The economic uncertainty faced by the United States, Canada, and other markets is only exacerbating the many other data protection risks that are threatening small businesses today. While businesses may be considering cutting technology or other budget line items to combat rising costs, decentralized working conditions are allowing cybercrime to evolve at an alarming rate. With the potential for longer-term cost savings and stronger customer retention, prioritizing data protection has never been more crucial.

After an all-time high of 1,864 data breaches in 2021, The ID Theft Center reports the number breaches remained stable, in 2022.[2] Impacting at least 422 million individuals, 1,802 total compromises in 2022 is notably higher than 2020's total of 1,108 compromises and the previous record of 1,506 compromises set in 2017. And while the number of breaches stayed level, the cost to businesses continues to rise. According to IBM, the average cost of a data breach reached $4.45 million globally in 2023 (vs. $4.35 million in 2022).[4] The United States had the highest average cost of a data breach at a staggering $9.48 million.[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. Given these ramifications, small business owners need to understand how data breaches occur and how to best prepare themselves.

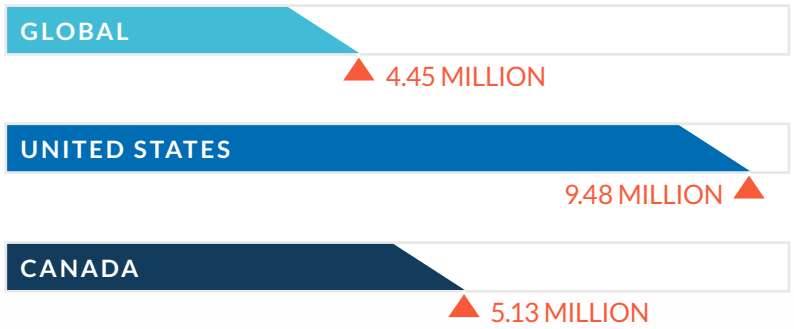
Report Definitions

For the purposes of this report, "data and information" are often referred to as distinct categories. Companies typically have and store both. Data includes raw, unorganized, and random facts, symbols, or figures (e.g., test scores, dates, salaries, etc.). Information is data that has been processed, interpreted, and structured in ways that are useful and meaningful. This gives context to the data.

Data breaches fall into two primary categories: physical and digital. Physical security breaches are a result of the theft of printed items such as proprietary business records, employee files, tax filings, customer information, and medical records as well as computing equipment. Digital security breaches can occur in many ways. This includes anything from deliberate attacks on a system or network that result in unauthorized access to oversharing as a result of human error. Developing a data protection strategy that prioritizes both digital and physical security risks is crucial in combatting data breaches.

Average Cost of a Data Breach By Country[4]

(Measured in U.S. $ millions)



Key Insights

Based on in-depth 2023 survey data and analysis of U.S. and Canadian small business leaders (SBLs) and consumers, Shred-it®'s 2023 Data Protection Report (DPR) reveals crucial insights on information security concerns and challenges today. It also reveals SBLs' perceptions of the current regulatory landscape and top concerns 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:

Vulnerable Small Businesses May Risk Losing Customers Following Breaches

Nearly three in four (73%) SBLs and almost all (94%) consumers surveyed are concerned about data breaches in the future. These concerns are even higher among Canadian small businesses than in the U.S. Nonetheless, only 60% of SBLs say they are proactive when it comes to data and information protection and a mere 22% report being 'extremely proactive', potentially leaving many small businesses exposed to the threat of a data breach. This has even declined from 2022, when 64% of SBLs reported being proactive. And despite consumers' significant concerns, most SBLs are not applying proactive approaches, like active monitoring or third-party risk assessments.

Training and Education Can Help Mitigate Potential Risks

IBM's 2023 Cost of a Data Breach Report shows that the costs of data breaches can be significantly reduced with employee training.[4] Just 15% of SBLs surveyed report that they require their employees to take any training, a stark decline from 2022. The few who do have mandatory training requirements are not offering training on a regular basis. A majority (63%) of SBLs admit they do not have a reliable source to maintain relevant policies and training, and 71% fear that their employees will not know what to do in the event of a breach. Such knowledge can help employees make better decisions to avoid breaches altogether or to minimize their financial impacts.

An Effective Compliance Strategy Can Benefit from a Strong Third-Party Partnership

The majority (76%) of SBLs surveyed worry that regulations will only become more complicated and burdensome for small businesses in the future. These worries are even more pronounced in Canada, where concerns about compliance are also very high. Sixty-seven percent of SBLs surveyed are even overwhelmed at the thought of changing procedures to meet existing regulations. There is a fear about not being able to keep up. Roughly half of SBLs do not currently have third-party partners to manage sensitive data and information, but 87% are likely to work with a subcontractor in the future. Almost all SBLs who do use a third-party partner for data security feel their partnerships are deeply valuable. Most desire support for their digital and/or physical data protection needs, which isn't surprising given the many stresses faced by small businesses.

The Misalignment of SBLs' Beliefs and Actions Regarding Data and Information Protection

More than **94% OF CONSUMERS** are concerned about having their personal information exposed by a data breach in the future

However, **71% OF SBLs** fear that their employees don't know what actions to take if a data breach occurs

More than **90% OF SBLs** believe that data and information protection and compliance trainings are an essential security practice

Yet, a Whopping **85% OF SBLs** do not require their employees to take any training on data and information protection

CURRENT DATA PROTECTION PRACTICES

With High Concerns About Data Breaches, Small Businesses are at Risk of Losing Customers

Small Businesses Recognize the Vital Importance of Data and Information Protection

The vast majority (92%) of SBLs surveyed believe that data protection has never been more important than it is today, and 93% reported that it is a top priority for their company. With the number of reported data breaches remaining very high according to the Identity Theft Resource Center's 2022 Data Breach Report,[2] this is not surprising.

Almost all (94%) of SBLs agree that physical data and information protection is just as important as digital data and information protection. Additionally, 43% of SBLs reported having spent more budget on data and information protection measures this year, which is encouraging. There is also a strong belief among small businesses that they are doing the right thing. In fact, most (90%) believe they have enough resources to keep sensitive data and information safe, and 89% are deploying the "best tools" to help keep organizational and customer data safe and protected. However, there seems to be a gap between these strong convictions and the reality of data protection practices at the ground level.

Percentage of SBLs that Allocated $5,000 or More For Data and Information Protection Purposes

79% in 2023

68% in 2022

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

> *"The high-profile data breaches in recent years have highlighted the need for stronger defenses, prompting increased budget allocations."*

> *"We want to take it more seriously this year and assure we have the best options available to our brand."*

Small Businesses Are Not Being Proactive in Their Approach, Leaving Data Protection to Chance

Despite the vast majority of respondents believing in the importance of data and information protection, most (78%) SBLs admit they are not taking an extremely proactive approach (even higher than last year). Canadian SBLs are even less likely to employ active measures such as frequent employee training and proactive monitoring, so it is not surprising that their fears and concerns are also higher. Yet, less than half (43%) of all SBLs report increasing their data protection budget allocations compared to 60% in 2022. More so than in 2022, 77% are afraid of impacting their customers due to a data breach and yet, they are taking mostly passive actions like software updates and anti-virus deployments to protect their sensitive data and information. Ninety-four percent of consumers are concerned about future breaches. Nonetheless, only 42% of SBLs (38% in the U.S. and 50% in Canada) have either updated their record retention policy three or more years ago or do not have this type of policy in place at all.

Furthermore, many SBLs are prioritizing digital risks and, as such, their organizations are left exposed and more vulnerable to physical risks. Only 25% of SBLs indicate that they collect and destroy sensitive materials when no longer needed (e.g., printed materials, 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.

Consistent with last year, digital risks were identified by SBLs as the most significant type of risk for data and information protection. This year, results show that nearly two-thirds of consumers also recognize the seriousness of digital risks. However, more consumers (45% vs. 28% of SBLs) view the sharing of data with third parties as a significant risk. This is another opportunity for small businesses to proactively address or highlight for potential customers the ways in which they are mitigating this risk.

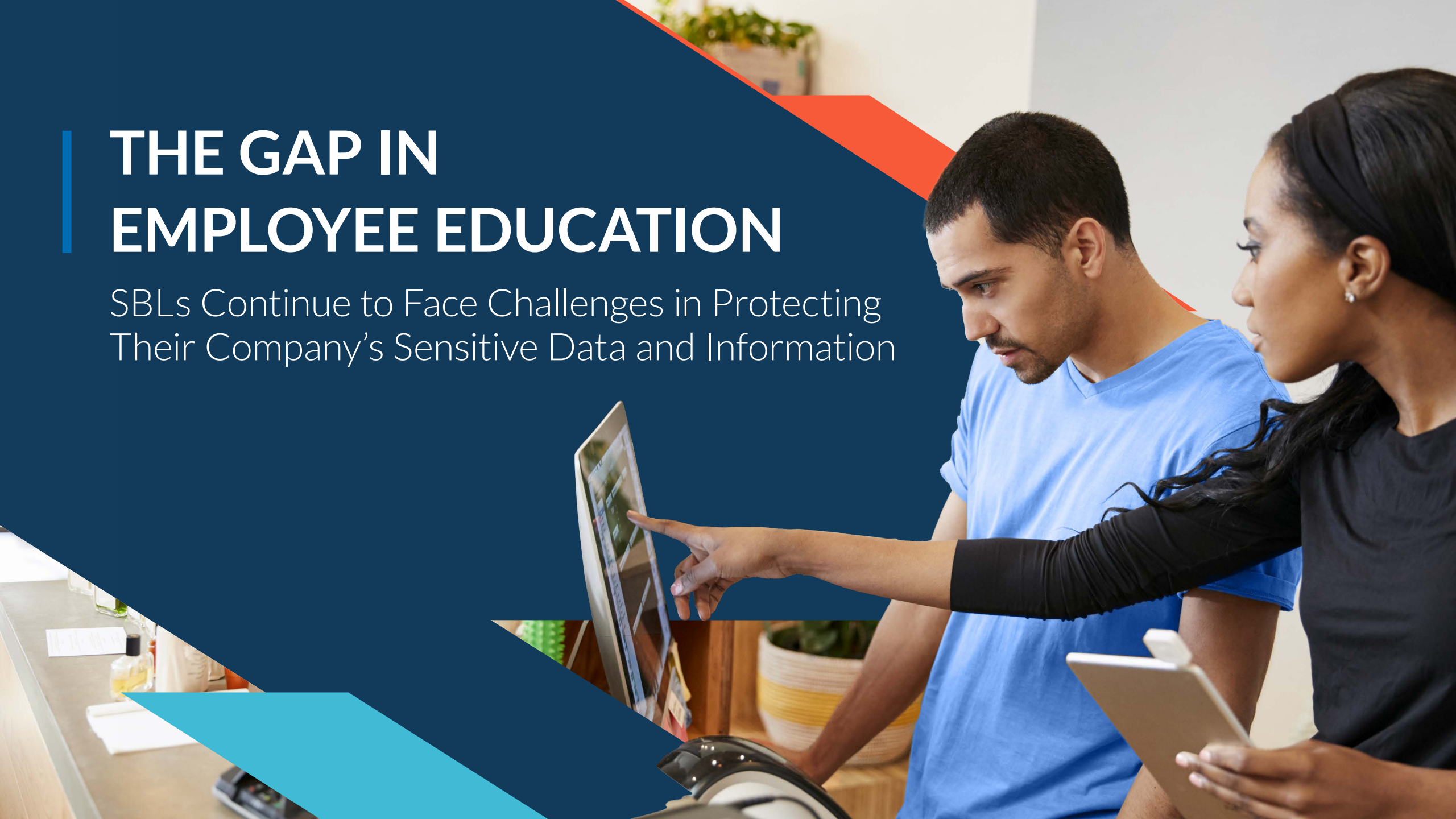
Actions Taken by Respondents to Keep Sensitive Data and Confidential Information Safe

PASSIVE MEASURES — ACTIVE MEASURES

- **20%** Implement audit or history logging of user access
- **16%** Conduct vulnerability assessments
- **30%** Deploy anti-virus programs
- **28%** Provide frequent software updates
- **21%** Conduct risk analysis/mitigation
- **19%** Implement and enforce record retention and destruction policies (e.g., Clean Desk, Shred-it-All)
- **17%** Hire employees who specialize in data and information protection
- **18%** Deploy automated security defenses to detect, investigate, and remediate data security threats
- **15%** Deploy third-party risk assessment programs
- **22%** Provide frequent data and information protection awareness training for employees (annually or more frequently)
- **22%** Put active monitoring programs in place
- **22%** Limit sharing of data with third parties (e.g., service providers, partners, suppliers)

THE GAP IN EMPLOYEE EDUCATION

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



There is a Clear Lack of Understanding About What Companies Need to Keep Themselves – and Their Customers – Better Protected Against Data Breaches

Despite their best efforts to prioritize and invest in data protection, the majority (73%) of SBLs surveyed admit it has never been harder to keep their company's sensitive data and information safe, and nearly three-quarters (also 73%) feel anxious or fearful about the safety of their company's data. These numbers are as much as 10% higher among Canadian small businesses whose fears are consistently more pronounced.

While only 26% of SBLs (23% in the U.S. and 34% in Canada) say they have experienced a data breach, this number is up since 2022. Additionally, 45% of consumers surveyed report experiencing a breach. Only 73% of SBLs are concerned about breaches in the future, significantly less than the 94% of consumers who worry about data breaches. Concerns are also higher among Canadian SBLs (81% vs. 70% in the U.S.).

Driving Factors of Small Business Owners' Data Protection Challenges and Concerns Today

68% EMPLOYEE TURNOVER | **66%** SUPPLY CHAIN VULNERABILITIES | **65%** REMOTE WORK

When asked about some of the key data and information protection challenges they experience as a small business owner, SBLs said:

"There are a lot of different types of threats to our sensitive data, and it is hard to find reliable security solutions."

"[It is a challenge] trying to stay on top of the best security and data safety networks and processes that there are available and keeping everything up to date."

"There are always people who are trying to scam via telephone or on the internet. Scammers are a big issue nowadays. They try to sell you fake products or information. Also getting hacked is a big issue. We had someone hack into our bank accounts last year. It was awful."

68% of U.S. SBLs	85% of CAN SBLs

~73% (Up 10% from 2022)

of **ALL** SBLs believe it's harder than ever to protect their company's sensitive data.

74% of U.S. SBLs	85% of CAN SBLs

~77% (Up 6% from 2022)

of **ALL** SBLs are afraid of impacting customers due to a data breach

73% of U.S. SBLs	81% of CAN SBLs

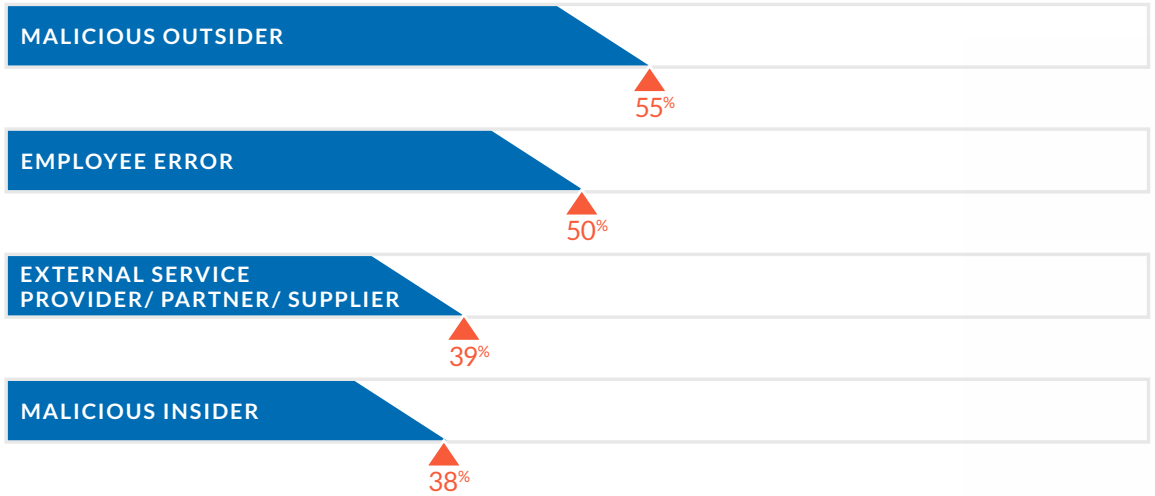
~76% (Up 5% from 2022)

of **ALL** SBLs are anxious about the safety of their company's sensitive data and information

SBLs Remain Concerned About the Employee Education Gap

Among the 26% of small businesses surveyed that have experienced a breach, 50% indicated that it was caused by employee error. According to Verizon's 2023 Data Breach Investigation Report, 74% of breaches this year involved a human element, including error, misuse, use of stolen credentials, or social engineering.[5] These mistakes can often result in considerable damage to organizations. The report describes the importance of equipping employees with enough knowledge about what to do when potential incidents arise, which can greatly improve a company's ability to combat them. Employees can be an important first line of defense because they are often easy targets for potential breaches.

Sources of Data Breaches According to Reporting SBLs



More than two-thirds of the SBLs surveyed worry that their companies do not offer enough training on data and information protection for all employees. Seventy-one percent fear that their employees don't know what actions to take if a data breach occurs. More than half admit that they – themselves – do not know what actions they should take. This is leading to high anxiety and fear about the future. In their own words, small business leaders cite a lack of education as an ongoing data protection challenge.

68% OF SBLs worry their company does not offer enough training on data and information protection for all employees

So, it is not surprising that **71% OF SBLs** fear that their employees don't know what actions to take if a data breach occurs

And **69% OF SBLs** fear that their employees don't know best practices to prevent a data breach

"I find it challenging to protect our company's sensitive data because of the lack of awareness about data protection amongst our employees."

– Small Business Leader

Despite Acknowledging its Importance, Most SBLs Do Not Enforce Data Protection Training for Employees

IBM's 2023 Cost of a Data Breach Report demonstrates that employee training can drastically reduce the total cost of a data breach.[4] Therefore, it isn't surprising that 92% of SBLs agree that data and information protection and compliance trainings are an essential security practice. However, in action, a mere 15% require their employees to complete such trainings. Even the few SBLs who do make education a requirement are not offering trainings with regular frequency.

"As a small business owner, I have inadequate training for data and information protection."

Company Requirements For Mandatory Data and Information Trainings

SBLs in the U.S. and Canada openly admit that they are facing challenges when it comes to employee training. Ninety-three percent wish they had a way to simplify their security training approach to properly educate their employees, and most (63%) lack a reliable source—be it internal or external—to consistently maintain their data and information protection policies and trainings. Both of these numbers have increased since 2022. Despite this, the vast majority (87%) feel they have the necessary resources to keep their employees trained in data and information protection requirements.

There is a realization among SBLs that their current training regimens and level of employee knowledge are not keeping pace with what is needed to keep their businesses well-protected. Although this does not appear driven by a lack of resources, there is a clear disconnect and a recognition that help—either internally or externally—is needed.

Fully **93%** OF **SBLs** (vs. 83% in 2022)

surveyed wish they had a way to simplify their security awareness training

More than **60%** OF **SBLs** (vs. 53% in 2022)

surveyed lack a reliable source (internal or external) to maintain data and information protection policies and trainings

THE REGULATORY LANDSCAPE

Changing Regulations Make it Difficult for Small Businesses to Stay Compliant

Trusted Partnerships Can Provide the Help SBLs Need to Navigate a Demanding Regulatory Landscape

Small Businesses Are Struggling to Keep Up in an Unpredictable Environment

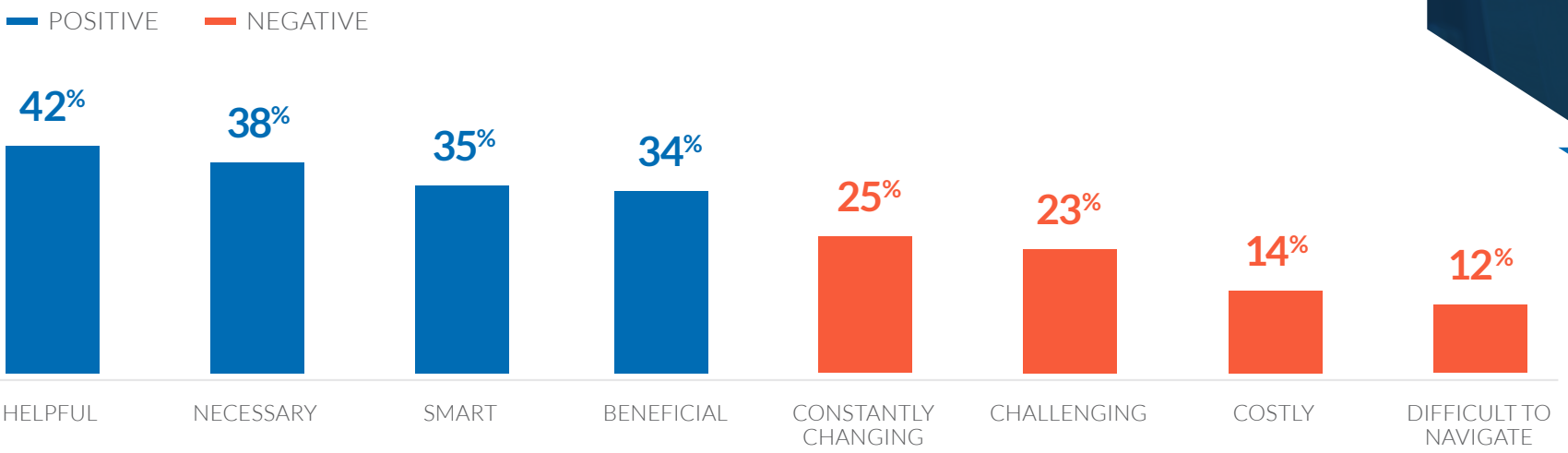
Most of the SBLs surveyed say they actively support new data and information protection regulations as efforts to advance consumer safety or sustainability. When asked to choose words to describe today's data and information protection regulatory environment, 42% stated that regulations are "Helpful" and 38% said "Necessary".However, close to half (49%) used a negative word to describe the environment, including "Constantly Changing", "Challenging", and "Costly". Those who perceive the regulatory environment negatively say it is because it is always challenging and increasingly difficult to stay up-to-date. Seventy-five percent agree that it will become harder to comply with regulations in the future.

When asked about today's data and information protection environment, some SBLs said:

"It's difficult to constantly adapt to changes and educate everyone on the importance of learning new techniques."

"I just don't think we can keep up."

Words Selected by Respondents to Describe Today's Regulatory Environment



In the current regulatory environment,

64% OF SBLs (60% in the U.S., 72% in Canada) feel they cannot keep track of changing regulations

Thinking about the future regulatory environment,

67% OF SBLs (63% in the U.S., 77% in Canada) feel overwhelmed by the thought of changes to existing regulations

Adding to their stresses,

64% OF SBLs (61% in the U.S., 74% in Canada) fear they won't be able to keep up with changing regulations in the future

Small Businesses Face Unique Regulatory Challenges

Adding to stresses and concerns, most responding SBLs agree that it is much more difficult for a small business to navigate changing regulations than it is for a larger one. These concerns also appear to be growing.

84% OF SBLs (vs. 83% in 2022) believe that larger businesses have an easier time complying because they have more resources

76% OF SBLs (vs. 75% in 2022) worry regulations will become more complicated and burdensome for small businesses in the future

81% OF SBLs (vs. 72% in 2022) agree that data and information protection regulations are tailored to large business

72% OF SBLs (vs. 67% in 2022) said that today's rules have created an unfair situation for small businesses

79% OF SBLs (vs. 72% in 2022) agree that small businesses are disproportionately affected by regulations

To Address Regulatory Changes:

52% OF SBLs are training employees on regulatory changes

51% OF SBLs are increasing or establishing dedicated internal teams

52% OF SBLs are actively monitoring changes to regulations (a drop from 60% in 2022)

40% OF SBLs are outsourcing to a third-party vendor or subcontractor

Likely due to a lack of support, many of the SBLs surveyed are not making any adjustments to address regulatory changes. For instance, only half say they are actively monitoring changes to regulations and just 4 in 10 are using a third-party to provide necessary support. It is not surprising that 66% of SBLs surveyed report they are not adjusting "very well" to changing regulations (even higher in Canada than in the U.S.).

66% of SBLs surveyed are not adjusting "very well" to changing data and information protection regulations

65% UNITED STATES

70% CANADA

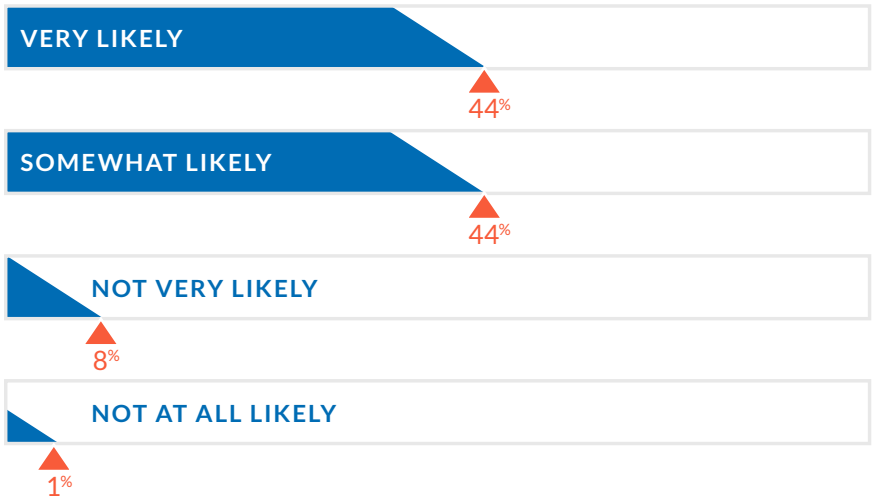
Small Businesses Can Rely on Trusted Partners to Provide the Support They Lack and Need

Collaborating with a trusted third-party security partner can help small businesses comply with the complex, burdensome, and shifting regulatory landscape. Currently, about half of SBLs surveyed are using a third-party vendor or subcontractor to help manage their company's sensitive data and information (53% digital and 46% physical). This group finds their partnerships deeply valuable. Almost all say that their partners help them comply with regulations and are confident that they fully understand this complex environment.

The majority of SBLs surveyed desire support from third-party partners and recognize that this is something they are lacking. They desire support for both training and for navigating the regulatory environment. Partnering with the right trusted third-party for data protection, management, and compliance can help SBLs gain more confidence in their organization's ability to protect their company's sensitive data and information.

Despite having higher concerns, a lack of adequate resources, and more trouble dealing with regulations, just 36% of Canadian SBLs say they would be 'very likely' to use a third-party vendor or subcontractor compared to 47% in the U.S.

Likelihood of Working With a Third-Party Vendor or Subcontractor to Manage Their Company's Sensitive Data and Information Protection Needs in the Future



63% OF SBLs do not have a reliable source (internal or external) to maintain data and information protection policies and trainings

61% OF SBLs do not have adequate support to navigate today's regulations (57% U.S., 69% Canada)

SBLs are most in need of support when managing their sensitive digital (60%) and physical (39%) data and information, strengthening current protection policies (30%), and providing continuous employee training and monitoring of compliance (26%).

60% OF SBLs need support in managing their sensitive digital data and information

39% OF SBLs need support in managing their sensitive physical data and information

30% OF SBLs need support in strengthening current protection policies

26% OF SBLs need support in providing continuous employee training for compliance

RECOMMENDATIONS: Stay Ahead or Risk Falling Further Behind

Security challenges for small businesses have increased with each passing year. SBLs should prioritize their data security efforts in order to help avoid a potential data breach. Steps that small businesses can take to help keep information and data safe include:

1. Protecting customers' sensitive data and information with proactive measures

Concerns in the wider population necessitate more proactive approaches for small businesses. Consumers are fearful of potential breaches even though more than half of those surveyed say they have never had their personal information exposed. Additionally, a future breach can potentially lead customers to spend their dollars elsewhere. Nonetheless, many SBLs continue to be reactive in their data protection efforts.

More needs to be done to allay internal fears, as well as those of potential customers. SBLs should consider providing regular data and information protection training to their employees. Proactive data and information security tactics such as active monitoring programs, a detailed risk analysis, and an active record retention and destruction policy (e.g., Clean Desk, Shred-it-All) can also help mitigate potential threats.

2. Closing the data protection knowledge gap

Small businesses need help training and educating their workforces around data protection best practices. SBLs are finding it harder than ever to protect their company's sensitive data and information, but their current training regimens and level of employee know-how are key soft spots that, if properly addressed, could significantly ease small business owners' data protection burdens and fears, and also help improve security. The SBLs surveyed recognize that more needs to be done but are not sure about how to achieve it.

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 (using either an internal or external source) 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 threats and risks and explain how to try to prevent a data breach in an approachable and engaging way.

3. Developing a partnership with a trusted third-party data and information protection provider

Though small business owners see the value in data protection regulations, the shifting regulatory landscape presents a complex, burdensome, and costly barrier to compliance. Those who currently work with third-parties recognize the value of those partnerships. Those who do not are open to starting these vital relationships in the future.

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 organization's needs.

> *"We need to have better protection because of news about data breaches."*
>
> – Small Business Leader

CONCLUSION

Small business leaders recognize that information and data security is paramount in building and retaining strong relationships with their customers. Many are at risk of losing customers if sensitive data and information becomes compromised. This represents significant potential revenue loss from which some small businesses may not be able to recover. Although smaller businesses struggle to match the comprehensive data security efforts of larger businesses, being proactive and allocating more budget up front can actually save money in the long run. There is an opportunity for small businesses to protect themselves from the very harmful effects of data compromises, and their customers expect them to take necessary steps to protect information.

Together, offering regular employee training and developing an understanding of the shifting data protection regulatory landscape are key to helping protect organizations from future data breaches. Enlisting the support of a trusted external partner can help guide small businesses through the complexities faced in these two areas. The right third-party partner can empower its clients, help to increase the confidence of SBLs and their employees to effectively mitigate the potential for future issues, and potentially minimize the impact of a breach should one occur. 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 that 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 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, our primary focus on document destruction 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 we can help you protect your organization.

We protect what matters.[SM]

Survey Methodology

This research was conducted through a 15-minute online survey to uncover small business leaders' information security concerns, challenges with data protection today, perceptions of today's data protection regulatory landscape and top barriers to compliance, the future outlook, and demand for external assistance from partners.

The audiences of focus for this research included small business leaders (e.g., business owners, executives, C-level, VP, Director+ or equivalent) who work at or own companies with 15-100 employees in the U.S. and Canada across a variety of sectors (e.g., healthcare, finance, professional services, insurance, real estate, etc.), as well as consumers (adults 18+) in the U.S. and Canada.

501
TOTAL SMALL BUSINESS LEADERS

350
IN THE U.S.

151
IN CANADA

NEW THIS YEAR

1,000
CONSUMERS

SOURCES

1. FBI Annual Report on Crime, 2009.
2. Identity Theft Resource Center, Annual Data Breach Report, 2022.
3. Ping Identify Consumer Survey, 2019.
4. IBM, Cost of a Data Breach Report, 2022.
5. Verizon, Data Breach Investigation Report, 2023.

Shred-it®
A Stericycle® Solution