10 YEARS

Shred-it®

DATA PROTECTION REPORT 2020

U.S. EDITION

Table of Contents

FOREWORD FROM CINDY MILLER, PRESIDENT AND CEO 3

EXECUTIVE SUMMARY 4

WITH DATA BREACHES ON THE RISE, CONSUMERS ARE LOSING TRUST IN DATA SECURITY 6

POLICY CREATION, POLICY ENFORCEMENT, AND TRAINING ARE CRITICAL DATA BREACH MITIGATORS 14

EMERGING TRENDS IN INFORMATION SECURITY 20

INDUSTRY-SPECIFIC INSIGHTS 23

- Healthcare 24
- Finance 25
- Legal 26
- Technology and IT 27
- Hospitality 28
- Automotive 29

THE EXPERT PERSPECTIVE 30

- Michael Borromeo, Vice President of Data Protection, Stericycle: The Evolution of Data Governance in the Wake of Digitalization 31
- Kelly McLendon, HIPAA Expert: Personal Health Information Protection in the U.S. Over the Past Ten Years 32

CONCLUSION: FINDING OPPORTUNITY 33

FOREWORD FROM CINDY MILLER

Today, businesses and organizations across the globe are more aware than ever of the importance of protecting data. Best practices for secure document management, digital data protection, and information security are still not well understood or widely practiced, yet are critical mitigators against data breaches. While digital data security awareness has grown, highlighted by public breaches at major corporations, physical data protection remains as important as ever.

Shred-it, a Stericycle service, helps organizations protect confidential information and prevent data breaches with secure paper shredding and media destruction services. In support of that mission, each year the Shred-it Data Protection Report (formerly known as the State of the Industry Report) sheds light on trends in data protection practices and the risks and opportunities businesses, organizations, and consumers face related to keeping their data secure.

Conducted by Ipsos on behalf of Shred-it, the report draws on detailed findings from an in-depth survey of C-suite executives (C-suites), small business owners (SBOs), and members of the public. The 2020 Data Protection Report (DPR) marks an exciting milestone with its tenth edition, where we distill the findings from our annual survey, highlight opinions of data security experts, and share insights and advice to help businesses, organizations, and consumers be better informed of data protection issues and better protected from the threat of data breaches.

As a society, we are facing new information security challenges every day. Business leaders must reevaluate employee training and protocols to adjust to our changing world and maintain consumer trust.

While completed prior to COVID-19, insights from the executives and consumers surveyed in this report highlight the need to have and enforce information security policies whether employees are working in the office or their homes. If there is one clear message in the 2020 data, it is that complacency around data protection creates significant risk for businesses. Over the past ten years, threats to data security have outpaced businesses' efforts and investments. As a result, all businesses should reevaluate their information security training and policies in earnest and focus on preparedness.

Shred-it is proud to stand alongside our clients and communities in this period of rapid change to help protect what matters. The world continues to change, but the need to protect what matters remains.

Cindy Miller
President and Chief Executive Officer
Stericycle

EXECUTIVE SUMMARY

The 2020 Data Protection Report (DPR) studies data protection beliefs and behaviors in a period of dynamic and rapid change. With insights gathered across ten years, it is evident that U.S. businesses are falling behind in several key data security practices.

The findings from Shred-it's in-depth survey of American C-suites, SBOs, and members of the public are distilled in this report—comparing this year's findings to those of previous years—along with an overview of best practices, industry research, and the opinions of data security experts. Continuing to build on previous research, this report highlights key themes:

- **The incidence of data breaches is highly prevalent (see page 9):** This year, 43% of C-suite business leaders reported a data breach, while 12% of SBOs did. The most commonly reported cause of a breach was the deliberate theft or sabotage by external vendors or sources, followed by human error, or accidental loss by an employee/insider.
- **Consumers are aware of data risks (see page 11):** 53% of consumers believe their personal data and information are *less secure* than they were 10 years ago and 86% are concerned that private, personal information about them is available somewhere on the internet.
- **Training and enforcement are lacking (see page 14):** 60% of C-suites and 46% of SBOs feel their organization has a policy for storing and disposing of confidential paper documents. However, 24% of C-suites and half of SBOs reported having no regular employee training on their information security policies or procedures.
- **Information security policies are needed for remote workers (see page 20):** Surveyed prior to the COVID-19 pandemic, 77% of C-suites and 53% of SBOs reported having employees who regularly or periodically work off-site. Shred-it research highlights the critical need for businesses to implement policies for storing and disposing of confidential information when employees work remotely.

Survey respondents comprised of:

100	903	2,011
C-SUITE EXECUTIVES (C-SUITES)	SMALL BUSINESS OWNERS (SBOs)	MEMBERS OF THE GENERAL PUBLIC ACROSS THE U.S.

Average Cost of Data Breach

$8.64 million

43% OF **C-SUITES** | 12% OF **SBOs**

have experienced a data breach

24% OF **C-SUITES** | 54% OF **SBOs**

have no regular training on information security procedures or policies

83% OF **CONSUMERS**

prefer to do business with companies who prioritize protecting their data

Read More »

Data Breaches Are the Result of Physical and Digital Risks

Data breaches can have devastating financial impacts on businesses, including legal fees, declining brand equity, the loss of customers, regulatory demands, and fines. It is critical that businesses act to both prevent breaches and minimize the impact should they occur.

Coupled with the high-profile data breaches seen this past decade, consumers are becoming increasingly skeptical that businesses can effectively self-regulate and govern a consumer protection framework.

Data Protection and Information Security Risks Fall into Two Primary Categories

Physical Risk
Theft of items or equipment such as:

Digital Risk
Unauthorized access, system or human error, or a deliberate attack on a system or network. Examples include:

62%
of Americans do not believe businesses report all data breaches

Compared to a decade ago:

53%
of Americans feel less secure about their personal data protection in 2020

With Data Breaches on the Rise, Consumers Are

LOSING TRUST IN DATA SECURITY

Read More

The Cost of Data Breaches Continues to Grow

The U.S. is facing a worrisome decline in information security compliance and vigilance. Businesses are more vulnerable to attacks than ever before. Given the high cost and other repercussions of data breaches, it is important that businesses develop corporate data security policies and practices that are strong and proactive.

According to research conducted by Ponemon Institute, the average cost of a data breach in the U.S. has risen substantially, climbing from

$3.54 million
in 2006

$8.64 million
in 2020

This research also shows that it pays to be prepared: businesses with an incident response team that extensively tested their incident response plan experienced $2 million less in data breach costs, on average, than those that had neither measure in place. The implementation of other measures, including working with an information security provider and providing regular security training for employees, can also significantly mitigate the costs of a data breach.

Data Privacy Is a Top Priority for Businesses

Perceptions of data breaches and data security reveal that privacy is a key concern among businesses. **Over 80% of business leaders surveyed indicate that data security is a top priority for them when choosing who to do business with**, and nearly all agree that companies need to do more to show how they are protecting personal information.

What Are the Biggest Threats Among C-suites?

1 in 4

perceive external threats from vendors or contractors

1 in 5

cite social engineering scams

1 in 5

indicate physical loss or theft of sensitive information

The majority of C-suites (83%) and SBOs (61%) are concerned that private personal information about their organization is available on the internet.

Businesses Anticipate Customers to Respond Negatively to Data Breaches

50% OF **C-SUITES** | **39%** OF **SBOs**

expect customers would demand to know what is being done to prevent future breaches

33% OF **C-SUITES** | **26%** OF **SBOs**

expect customers would tell others about the breach

42% OF **C-SUITES** | **22%** OF **SBOs**

expect customers to seek compensation for the breach

Recognizing the threats and consequences of data breaches, leaders of businesses of all sizes are making significant investments in data security.

Impact of Data Breaches on the Rise

According to the Risk Based Security Data Breach Report, there were over 7,000 publicly reported breaches in 2019, exposing more than 15.1 billion records. Their research indicates that the number of **reported breaches** in Q1 2020 decreased compared to Q1 2019, though the number of **exposed** records was higher in Q1 2020. According to the report, the decline in disclosed breaches can be attributed to reporting disruptions brought on by the COVID-19 pandemic and unusually high number of breaches reported in Q1 2019.

Businesses Are More Vulnerable Than Ever

65% OF **C-SUITES** | **31%** OF **SBOs**

report that their organization is likely to suffer a data breach within the next 5 years

43% OF **C-SUITES**

experienced a data breach *(up from 32% in 2018)*

12% OF **SBOs**

experienced a data breach *(up from 3% in 2018)*

Cause and Detection of DATA BREACHES

57% OF **C-SUITES** | **71%** OF **SBOs**

say it took their organization a week, or longer, to detect the breach

31% OF **C-SUITES** | **36%** OF **SBOs**

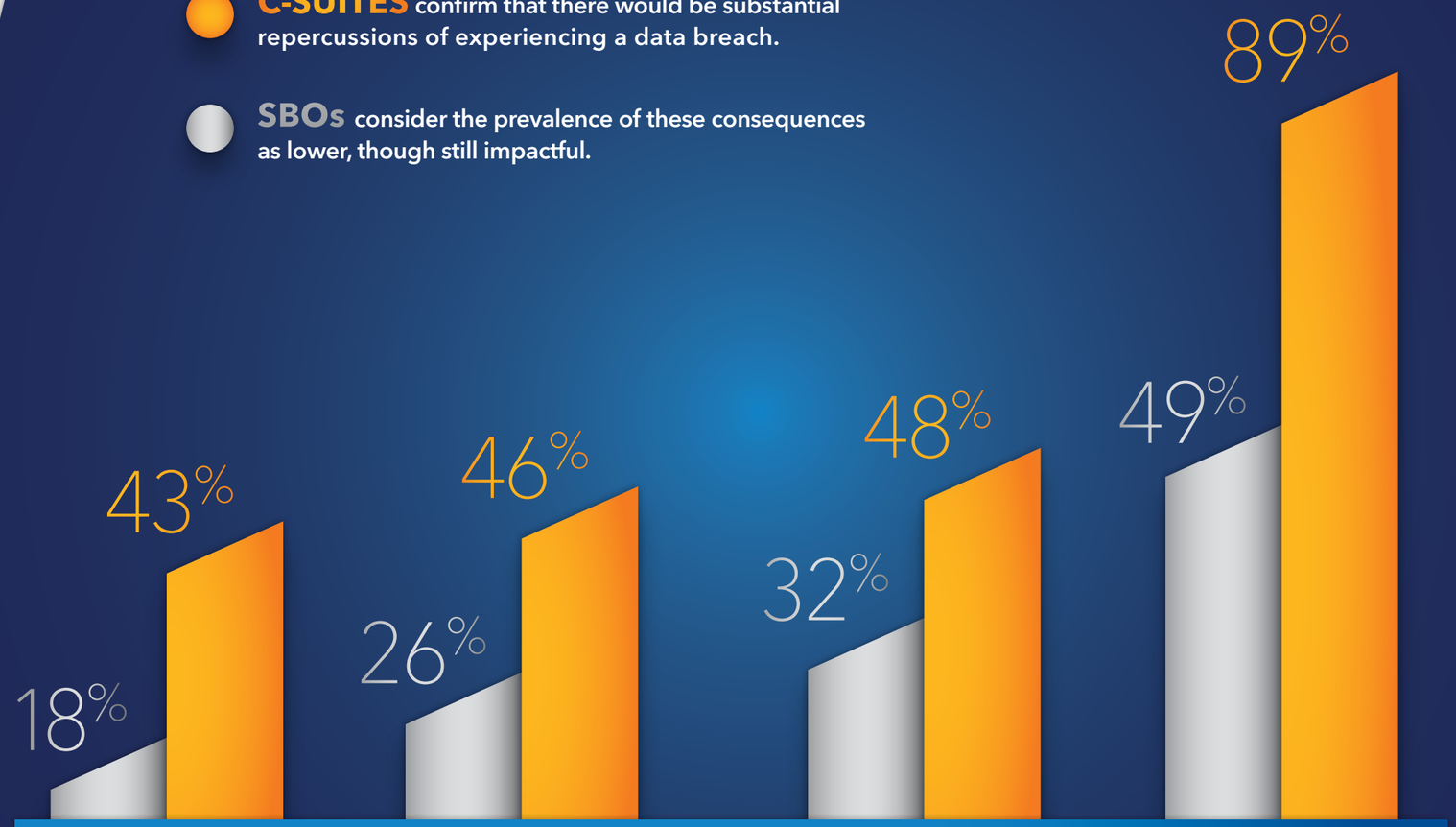
attributed the breach to deliberate theft or sabotage by external vendors or sources, followed by human error or accidental loss by an employee/insider

Negative Impact of Data Breaches Increasingly Known by Business Leaders

Survey findings show that businesses understand the importance of safeguarding sensitive information and the potential ramifications.

C-SUITES confirm that there would be substantial repercussions of experiencing a data breach.

SBOs consider the prevalence of these consequences as lower, though still impactful.



Consumer Perceptions and Expectations

While consumers accept the reality of data breaches, they demand transparency and a decisive response when it happens. They take the issue seriously and want to know if and when a data breach happens. This is an expectation that business leaders acknowledge they are not always delivering on.

When data breaches occur, consumers will wait to see how the affected company reacts to the situation before they decide how to proceed.

Many consumers maintain very low expectations of businesses around data security. A majority of consumers surveyed do not trust that all data breaches are reported and continue to be concerned that their own private, personal, and sensitive information exists somewhere on the internet.

Today, consumers are twice as likely to feel less secure about their personal data security than they did ten years ago.

This suggests a greater awareness amongst consumers of the everyday presence of security threats and privacy risks. It may also point to an understanding among consumers of the growing sophistication of cyber attackers. As the two privacy experts assert in *The Expert Perspective* section of this report, the cyber attackers of today are far more sophisticated than the ones of the past. Organizations have a critical responsibility to protect the data they use and that of consumers.

Consumer Perceptions and Expectations (continued)

High Concern about Data Privacy

- Those who fall under the age of 35 are least likely to express concerns about their information being on the internet (81% vs. 88% for older generations) or in paper formats (63% vs. 72% for older generations).
- 83% indicated that physical and digital data security is a top priority for them when choosing who to do business with.

83%
OF CONSUMERS
feel that data breaches are very serious events

Low and Falling Trust in Data Security

- 86% of consumers are concerned that private, personal information about them is present on the internet.
- Only 38% of consumers trust that all physical and digital data breaches are adequately disclosed to consumers.
- 45% of employees perceive a data breach as being at least somewhat likely to occur within the next five years in the organization they work for.

53%
OF CONSUMERS
believe their personal data and information are less secure than they were ten years ago

Consumers Take Action When Expectations Aren't Met

- 55% of consumers responded that they will wait and see how a company will react to the situation before determining how to respond.
- 29% of consumers will tell others about a breach.
- 24% of consumers will stop doing business with a company if their personal information was compromised in a data breach.

31%
OF CONSUMERS
would lose trust in a company and demand to know what it is doing to prevent future breaches

Consumer Privacy and Security Bolstered through Expanded Legislation

Legislative requirements have also evolved over the past decade with expanded privacy and security protections, as well as greater consequences for non-compliance. These changes are global in scale, ranging from the GDPR in Europe to the CCPA in California. The U.S. continues to lack an integrated federal data security and privacy legislative framework.

This timeline highlights key legislative changes impacting American business and organizations.

Please note: This timeline is not comprehensive and provides only a general overview.

2013

The Health Insurance Portability and Accountability Act (HIPAA) Omnibus Rule came into effect on January 25, 2013. It signaled the final modifications to the privacy and security rule within the Act and also contained changes for enforcement, breach notification rules, and the **Genetic Information Nondiscrimination Act (GINA).** This act is designed to prohibit some types of genetic discrimination, including barring the use of genetic information in health insurance and employment.

2018 – 2019

Europe's General Data Protection Regulation (GDPR) has implications for American business and organizations, particularly those controlling or processing personal information in the European Union (EU) or the information of EU citizens.

The **United States-Mexico-Canada Agreement (USMCA),** the successor to NAFTA, was announced and includes a Digital Trade chapter that addresses personal information protection, cross-border transfer of information by electronic means, and location of computing facilities.

With the passing of the **Alabama Data Breach Notification Act** of 2018 (SB 318), all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals when their personally identifiable information is exposed as a result of a data breach.

Specific to New York, **the Stop Hacks and Improve Electronic Data Security (SHIELD) Act** is enacted July 25, 2019. The law augments existing federal protections around consumers' private information, holding accountable any company that does business within the state.

2020

The **California Consumer Protection Act (CCPA)** comes into effect and applies to businesses that collect, use, and disclose the personal information of California consumers, even if the businesses are not physically located or have employees in California.

The Office of the Privacy Commissioner of Canada launches consultation on artificial intelligence (AI) as it relates specifically to PIPEDA, as part of the federal legislative reform policy analysis.

Several other states are using **CCPA** as a model and are including state-specific nuances. This includes Illinois' Data Transparency and Privacy Act (HB 3358) (came into effect January 1, 2020), Massachusetts' Consumer Privacy Bill (S.120) (pending), the New York Privacy Act (S5642) (pending), the Virginia Privacy Act (HB 472) (came into effect January 8, 2020), New Hampshire's HB 1680-FN (goes into effect January 1, 2021), and Florida's **CCPA** companion bill (came into effect July 2020).

Policy Creation, Policy Enforcement, and Training Are

CRITICAL DATA BREACH MITIGATORS

Read More

Insufficient Focus on Employee Training

Despite the high number of data breaches in 2020, businesses are not prioritizing policies for disposal of confidential information as much as they did in previous years.

Information Security Policies

60% OF **C-SUITES** | **46%** OF **SBOs**

have a known and understood policy for storing and disposing of confidential paper documents, and the policy is strictly adhered to by all employees

27% of C-suites and 15% of SBOs have a policy, but not all employees are aware of it

10% OF **C-SUITES** | **38%** OF **SBOs**

do not have a policy for disposing of confidential paper documents

67% OF **C-SUITES** | **36%** OF **SBOs**

have a known and understood policy for storing and disposing of confidential information on end-of-life electronic devices, and the policy is strictly adhered to by all employees

21% of C-suites and 13% of SBOs have a policy, but not all employees are aware of it

10% OF **C-SUITES** | **49%** OF **SBOs**

have no policy for disposing of confidential information on end-of-life electronic devices

Policy Best Practices

Best practices for storing and disposing of confidential information include having a *Remote Work Policy* that outlines how employees should store and dispose of confidential information while working off-site, implementing a *Clean Desk Policy* that specifies how everyone should manage their workspace to protect sensitive information, and creating policies for the secure destruction of paper documents and electronic media.

Guidelines for **SECURE DOCUMENT DESTRUCTION** include:

- Implementing a *Shred-it All* policy to standardize document destruction procedures across an organization and avoid the risks of human error or poor judgment about what needs to be shredded
- Shredding before recycling to reduce the chance that unattended paper could leave an organization vulnerable to security breaches
- Storing all documents to be shredded in a secure console
- Shredding using a reliable professional service with a secure chain of custody that includes on-site destruction

Guidelines for **SECURE MEDIA DESTRUCTION** include:

- Implementing a secure destruction policy of electronic media, such as hard drives and digital information, is the only way to ensure that a data breach does not occur
- Avoiding stockpiling old electronic media and regularly cleaning out storage facilities
- Using a secure method to dispose of hard drives and electronics before materials are recycled
- Working with a specialist who maintains a tight chain of custody to ensure the secure destruction of electronic media

SBOs Lag in Adoption of Cyber Insurance

There is a growing market for cyber insurance, which offers businesses important protection against the loss, theft, or destruction of their digital assets. Cyber insurance policies help businesses cover financial losses and expenses related to breaches, such as those from ransoms, forensics work, legal assistance, recovery, and the costs of disruption. North America is currently the largest market for cyber insurance and rapid growth is expected to continue as businesses become more aware of the risks of cyber losses. While cyber insurance cannot protect a business from cybercrime, it can certainly help to prevent devastating financial impacts should a cyber incident occur.

While C-suites more frequently reported having a cyber insurance policy in place than SBOs, research shows that small businesses are not immune from the threat of cybercrime. Symantec's 2019 Internet Security Threat Report indicated that smaller organizations were more likely to be hit by email threats—including spam, phishing, and email malware—than larger organizations.

84% OF **C-SUITES**

33% OF **SBOs**

reported having a cyber insurance policy in place to protect against data breaches

Despite Risks, Employee Training on Information Security Procedures Is Inadequate

With one of the most common causes of data breaches being employee error, providing training that keeps employees informed about data security policies is critical to lowering organizational risk.

> Building a culture of information security and privacy compliance requires strong employee training.

24% OF **C-SUITES** | **54%** OF **SBOs**

reported having no regular employee training on information security procedures or policies

55% OF **C-SUITES** | **27%** OF **SBOs**

reported that their employees receive training in information security at least twice a year

45% OF **C-SUITES** | **20%** OF **SBOs**

conduct random security checks and subject employees to spur-of-the-moment office walkthroughs

While some businesses have training in place, the survey results highlight the need for improvement and a **heightened awareness of the role employees play in safeguarding information.**

Lack of Training on Confidential Document Policies Increases Security Risks

Although more than half of C-suites and nearly half of SBOs have a known and understood policy for storing and disposing of confidential paper documents, survey data suggests that proper reinforcement of these policies is necessary to reduce security risks.

Establishing information security policies is an important step, but businesses should also ensure that all employees are trained on a regular basis. Employee training can go a long way in preventing breaches by human error, growing awareness of data security, and building a workplace culture of security. Ponemon Institute's 2020 study on the costs of data breaches revealed that employee training was a significant mitigating factor in reducing the total cost, decreasing the average cost of a breach by $238,019.

An information security program should include training on the secure disposal of paper documents. This training should ensure employees understand the importance of securely destroying documents, covering what needs to be shredded, and at what intervals, as well as how confidential documents should be stored. Employees should get regular training refreshers and all new hires should go through training during their onboarding process.

3 in 10 EMPLOYEES

do not make any effort to shred mailing labels and personal information

63% OF **C-SUITES** | **31%** OF **SBOs**

report that their employees have left confidential documents out in the open

80% OF **C-SUITES** | **61%** OF **SBOs**

report that their employees default to printing documents that need to be reviewed or signed

62% OF **C-SUITES** | **38%** OF **SBOs**

use a locked console in the office and either an in-house or a professional shredding service to dispose of confidential documents

19% OF **C-SUITES** | **32%** OF **SBOs**

use a shredding machine but no locked console to secure confidential documents prior to shredding

Training Needs to Incorporate New Cyber Threats

Interestingly, this year's report uncovered that the number of organizations that regularly train their employees on how to identify common cyber-attack tactics such as phishing, ransomware, or other malicious software has declined, creating space for American companies to do more. As the sophistication of cyber-attackers grows, so too does the need for more frequent and thorough employee training.

> Employee training plays a vital role when it comes to proper protection practices and combating external risks.

82% OF **C-SUITES**
(down from 88% in 2019)

45% OF **SBOs**
(down from 52% in 2019)

state that their employees receive regular cyber-attack training, designed to help them identify phishing, ransomware, or other malware

64% OF **INDIVIDUALS**
surveyed **reported that they were targeted by a phishing email** or social engineering scam attempt in the workplace

11% OF **EMPLOYEES**
fell victim to it

1 in 5 EMPLOYEES
use the **same password** for every login

1 in 3 EMPLOYEES
admit to **saving their passwords in a list on their computer** or mobile device

EMERGING TRENDS

in Information Security

Read More

Maintaining Information Security While Working Remotely

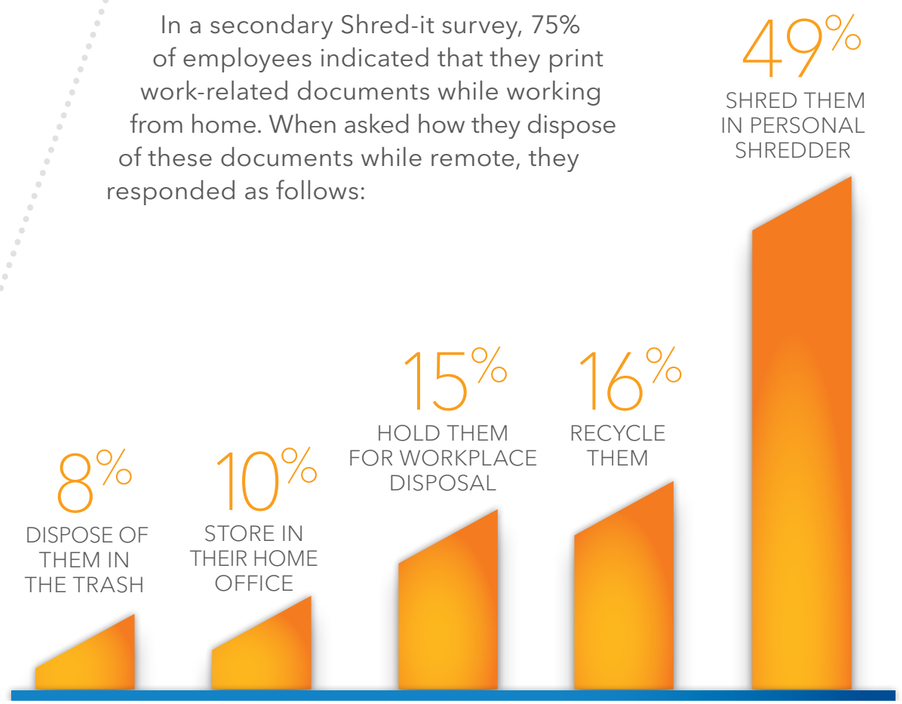
While the work-from-home trend has risen steadily across all industries over the past decade, the recent COVID-19 pandemic abruptly launched employees into work-from-home mode. With remote work, many organizations—with or without supporting policies—put themselves at an increased data security risk, especially when human error and physical document handling are taken into consideration, as many employees rely on printed copies of documents containing confidential information.

> When working remotely, employees should shred their paper, take it back to the office, or drop it off at a local paper shredding company.

This year's survey reinforced the need for vigilance versus complacency. More than ever, businesses must take a more proactive approach to implement proper training and data security protocols for all employees, regardless of their location.

Prior to the pandemic, **77%** OF **C-SUITES** AND **53%** OF **SBOs** had employees who regularly or periodically work off-site

In a secondary Shred-it survey, 75% of employees indicated that they print work-related documents while working from home. When asked how they dispose of these documents while remote, they responded as follows:



53% OF **SBOs** have a policy in place for storing and disposing of confidential information when employees work off-site or away from the office, however only **41% of organizations** indicate that their **policy is strictly adhered to by all employees**

45% OF **SBOs** state that **no policy** exists at all

Myth or Fact: The Paperless Office

Although there has long been talk of the paperless office, businesses still consume paper. Barriers to the paperless office include both technical obstacles along with habits and personal preferences, such as the desire to hold and mark up paper.

Rather than pursue the goal of the paperless office, businesses would be wise to make optimal use of both paper and electronic documents and ensure that policies are in place for secure storage and disposal, no matter the working location of employees.

7% OF **C-SUITES** | **18%** OF **SBOs**

operate in a paperless office environment

INDUSTRY-SPECIFIC INSIGHTS

The 2020 DPR includes an in-depth review of industry-specific practices throughout the healthcare, finance, legal, technology and IT, hospitality, and automotive industries. While each has unique realities, they share a sense of complacency around information security and a lack of preparedness for the increase in remote work observed over the past few years, particularly in 2020.

When asked about data and information security, leaders of most industries are aware of, and concerned about, the risk of a breach to their organization. The challenge, they acknowledge, is a gap in turning concern into action.

> **Many organizations still lack a cyber insurance plan and could be caught off guard in the event of a breach.**

Read More »

Healthcare

Health Insurance Portability and Accountability Act (HIPAA) regulations continue to create high adherence in healthcare employees to secure private patient information properly.

With this context, healthcare organizations need to continue to react and evolve and will be required to maintain stringent security protocols to protect Americans' private health data.

Key 2020 Findings

- Only 14% of healthcare organizations have gone paperless, and 16% have access to a professional shredding service.
- Healthcare organizations need to increase information security training, with 20% stating that employees never receive training during their employment and 18% reporting that employees receive training only once.
- Data breaches are anticipated in the healthcare industry with 42% of organizations concerned they will experience a breach within the next five years.
- Additional security threats can come from additional sources that need safeguards. Healthcare organizations believe the biggest information security threats they will face include external threats from vendors (18%), physical loss or theft of sensitive information (17%), and insider threats from employees (rogue employees) (16%).
- 91% of healthcare organizations agree that companies need to do more to show employees and consumers how they are protecting personal information.

Finance

This year's report uncovered that nearly half of the financial services professionals surveyed believe they are at risk of a data breach. This, and the fact that the industry processes a large amount of private data, makes it more important than ever to have strong information security policies in place.

Shred-it's 2020 Data Protection Report reveals that remote work is becoming increasingly important in the financial industry. However, some financial organizations are not prepared for the potential threats to their business, employees, and most importantly, their customers.

Key 2020 Findings

- Nearly 3 in 5 (59%) C-suites and SBOs in the financial services industry say their employees work off-site on a regular basis.
- However, more than 1 in 4 (27%) financial services professionals say their organization does not have a known and understood policy for storing and disposing of confidential information when employees work off-site/away from the office.
- Nearly 9 in 10 (85%) financial services professionals believe the option to work remotely is going to become increasingly important to their employees in the next five years.

21%

OF FINANCIAL SERVICES COMPANIES

admit they have suffered a data breach

Legal

Court systems lag in technology adoption overall, with many continuing to rely on paper-based practices, including physically signing documents and printing hard copies. This creates unique vulnerabilities for this sector, and in 2020, physical loss or theft of sensitive information remains the highest risk for this industry.

The highly-confidential nature of legal information requires continued diligence of employees to maintain policies. This industry, which relies on relationships and quality client service, needs to understand that data security is both a relationship management and a client service function.

Key 2020 Findings

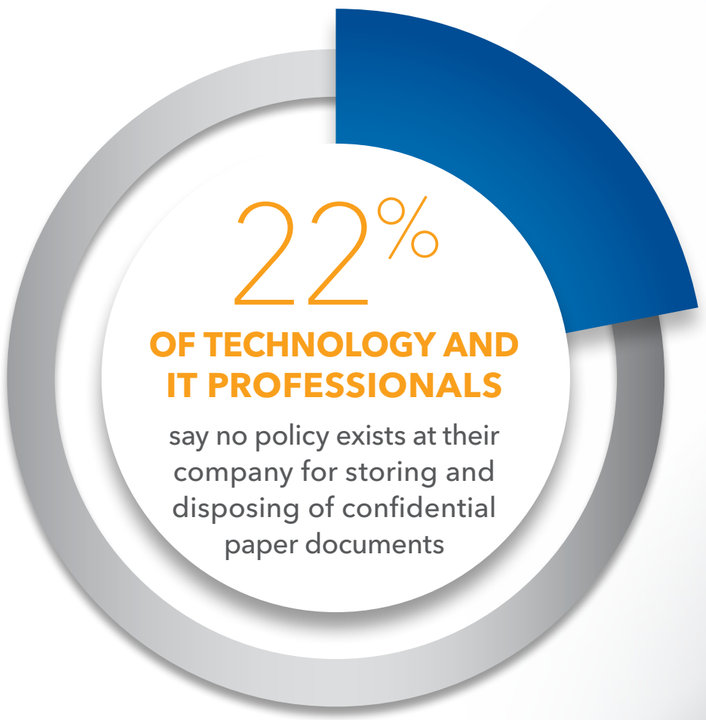
- Nearly one quarter (22%) of security threats to legal businesses stem from physical loss or theft of sensitive information and external threats from vendors or contractors (22%).
- Only 6% of legal businesses indicated that their offices are paperless, suggesting that they still work with a significant amount of paper copies that include confidential information.
- 79% of legal business employees default to printing documents that need to be signed or reviewed and 43% have left confidential documents on their desks or out in the open.

Technology and IT

The technology and IT industries are among the most advanced when it comes to having clear and understood policies for storing and disposing of confidential paper documents.

> The 2020 DPR reveals gaps showing this industry is **not instituting employee training at the level it should be**.

Many employees agree that companies need to do more to demonstrate their data protection policies, exposing a vulnerability as this industry maintains a strong work-from-home segment.



Key 2020 Findings

- Nearly a third (30%) also say no policy exists at their company for storing and disposing of confidential information on end-of-life devices; while 17% have a policy, not all employees are aware of it.
- 94% of technology and IT businesses agree that companies need to do more to show employees and consumers how they are protecting personal information.
- 67% of employees at technology and IT businesses work off-site or away from the office regularly; however, 23% of businesses do not currently have a policy for storing and disposing of confidential information when employees work off-site.
- While 70% of technology and IT businesses are concerned that private, personal information about their organization is out on the internet somewhere, 29% of them believe that data breaches are not serious and are blown out of proportion.
- 68% of technology and IT employees default to printing documents that need to be signed or reviewed, and 47% have left confidential documents on their desks or out in the open.

Hospitality

Amid the recent COVID-19 pandemic, the hospitality industry is experiencing challenging times. With closed doors or limited service, there will be a new focus on ensuring guests are safe when business resumes. With this said, data security measures and training are more important than ever as the industry works to rebuild its overall reputation for being safe and secure coming out of this health crisis.

Hospitality organizations have identified an increase in employees working away from the office and a lack of preparedness to address the security concerns that come with this new way of working.

> **The 2020 DPR noted a gap in training and policy awareness**, with few organizations in this sector having work-from-home policies covering both tactics and procedures.

The hotel industry needs to ensure staff are trained on how to identify phishing, ransomware, or other malware attacks so that private guest information and other sensitive data does not end up on the internet or in the wrong hands.

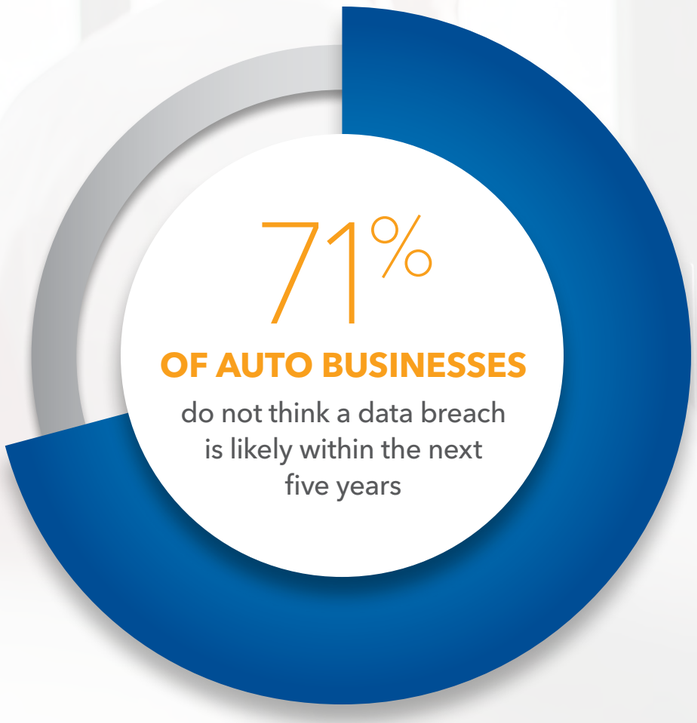
Key 2020 Findings

- 28% of hospitality businesses do not train employees on how to identify common cyber-attack tactics such as phishing, ransomware, or other malware (malicious software), and 27% conduct training, but only once.
- Almost two-thirds of employees work off-site or away from the office on a regular basis (70%), yet 26% of C-suites and SBOs confirm that no policy exists for storing and disposing of confidential information when employees work off-site or away from the office.
- While 62% of hospitality businesses are concerned that private, personal information about their organization is out on the internet somewhere, 42% of them believe that data breaches are not serious and are blown out of proportion.

Automotive

With approximately 17 million cars sold across the U.S. in 2019, dealerships handled a corresponding seventeen million credit scores, drivers' licenses, insurance information, and other personal data. Despite this reality, tremendous complacency was observed in this industry when it comes to placing themselves at an increased risk of experiencing a data breach.

> As an industry that relies on **reputation and relationship building**, similar to that of a financial institution, **data security must be a main pillar of client service**.



Key 2020 Findings

- 29% of auto businesses do not train employees on how to identify common cyber-attack tactics such as phishing, ransomware, or other malware (malicious software); and 14% conduct training, but only once.
- While 66% of auto businesses are concerned that private, personal information about their organization is out on the internet somewhere, 24% of them believe that data breaches are serious.
- 43% of employees work off-site or away from the office on a regular basis, yet 43% of C-suites and SBOs confirm that no policy exists for storing and disposing of confidential information when employees work off-site or away from the office.

THE EXPERT PERSPECTIVE

Read More

THE EXPERT PERSPECTIVE

Michael Borromeo,
Vice President of Data Protection, Stericycle

The Evolution of Data Governance in the Wake of Digitalization

Over the last decade, data protection laws and regulations have undergone a stark evolution to not only deter the criminal, but also compel organizations to act. These laws now have "teeth" in terms of coverage and consequences for non-compliance that require organizations to think critically about the impact of data on their business and what steps are needed to protect it.

> While there is still a long way to go, businesses across the globe are finally beginning to grasp the importance of privacy and cybersecurity issues.

Moreover, businesses realize that they are not immune to backlash as a result of a data breach. For instance, consumers have made it clear that they expect their data to be protected, and Boards of Directors have not hesitated to replace C-suite executives when the neglect of cybersecurity has caused company embarrassment, brand damage, or financial losses.

Unfortunately, while many organizations work to develop their data protection practices, criminals have also continued to improve at their craft as well.

> Attackers have evolved from simply motivated individuals into coordinated crime syndicates and nation-state sponsored cyber warfare groups.

Consequently, the sophistication of their attacks has grown, and any organization can become a target.

Malicious software, also known as malware, continues to challenge organizations. In many cases, well-funded organized crime entities can have better software development processes than the corporations they are attacking, which is why their malware is so effective and destructive. Ransomware can be particularly devastating, as it forces organizations to answer the ultimate question, "To pay, or not to pay?"

In the coming years, Artificial Intelligence (AI) will also have important implications for cybersecurity. While AI has many useful applications, it unfortunately can also be used for nefarious purposes. We will likely begin seeing AI used to create deep fakes to aid in social engineering, which may lead to an increase in the successful distribution of malware and ransomware as well as breaches of personal data.

> As data grows exponentially year over year and the security and privacy landscape evolves, the cybersecurity battle will continue to escalate. As a result, organizations must continue adapting security measures to ensure they are protecting the data they use, process, store and share.

Properly fulfilling these responsibilities is not only important for a company's long-term sustainability, but it's also important to the people from whom they've collected it.

THE EXPERT PERSPECTIVE

Kelly McLendon,
RHIA, CHPS – HIPAA Expert

Personal Health Information Protection in the U.S. Over the Past 10 Years

In recent years, personal health information protection has emerged into greater prominence given the rise of healthcare data breaches, including cyber and ransomware attacks on healthcare providers and insurers. In the U.S., the Health Insurance Portability and Accountability Act (HIPAA) is the most comprehensive federal legislation that provides data privacy and security provisions for safeguarding healthcare information, including protecting sensitive patient health information from being disclosed without a patient's consent or knowledge.

While individuals' personal health information is more secure now than it was in the past, the adversary hackers are better too.

> Today, there is far more electronic patient health information and its data footprint is much larger than ever.

Hackers are also targeting the healthcare industry more than ever in the past. HIPAA has undergone significant changes in the past ten years but remains the leading source for expansive healthcare privacy protections. HIPAA privacy laws changed markedly in 2013 with the Omnibus Final Privacy Rule, mostly in areas surrounding breach analysis and clarification of a business associate coverage and liability. Between 2016 and 2020, there was a set of challenges in understanding how to respond to patients' access to information requests that has only recently been resolved.

Most recently, the Office of the National Coordinator of Healthcare IT (ONC) has issued new rules about interoperability and information blocking, which will present new challenges in determining the required changes to policies, procedures, workforce training, and compliance. These rules are being delayed 90 days due to COVID-19 but must be prepared for as quickly as possible given the potential large magnitude of change that may be introduced in the Protected Health Information (PHI) disclosure processes.

COVID-19 has also spawned new rule making in reference to alignment of 42 CFR Part Substance Abuse records with HIPAA. In general, these rules are moving towards uniformity with HIPAA, but the final rules will need to be published prior to implementation later this year or in 2021.

Also, attention has turned to new privacy laws that have emerged with the California Consumer Protection Act (CCPA) and the EU's General Data Protection Rule (GDPR). These pieces of legislation widen the scope of personal information that is managed by laws and rules, beyond what HIPAA covers. This expansion could be challenging to implement, especially if there is no federal privacy law and instead various privacy laws at the state level.

Increasingly, privacy compliance will impact healthcare system operations as entities work to keep various types of personal data confidential and to protect individuals' identities. Looking forward into the future, privacy will be more highly regulated, which will mean increased patient control and attention given to the privacy of their personal information, which is good for everyone except those who try misuse the data.

CONCLUSION

Finding Opportunity

Shred-it's 2020 Data Protection Report presents a wake-up call for U.S. business leaders.

> **Reduced focus on policies and training has created an environment whereby employee and customer data are at risk.**

The 2020 DPR confirms that businesses, both large and small, need to remain vigilant in the ever-changing and adapting data protection landscape. Businesses must continue to invest in training to ensure that all employees, on or off-site, can maintain the same level of security and protection to the private, personal information they encounter in their day-to-day roles.

Throughout the 2020 report, four prominent themes emerged:

- **Reinforcement of policies necessary:** In an effort to mitigate security risks, businesses should monitor and address employee compliance of confidential information policies.
- **More regular training needed:** While some organizations having training programs in place, more can be done to keep their employees and company safe through regular training and program refreshers.
- **Remote work unpreparedness:** Working remotely has become an essential routine in most Americans' lives, but information security policies have not caught up.
- **Lack of consumer trust:** Consumers' declining trust in businesses threatens to impact bottom lines.

> **A volatile and changing environment requires a focus on preparedness, training, and policies to ensure the safety of American consumers and businesses.**

With data and documents distributed like never before, there is an urgency to act now, before these risks are realized. It is time for businesses to invest and lead in data protection.

> **An urgent focus in training and policy development will help employees protect sensitive business and customer data from cyber-attacks and minimize risks around physical documents.**

Businesses can set up long-term practices that benefit and protect against future risks. Shred-it has the expertise and experience to be part of the solution and is committed to helping protect and safeguard data, reputation, and businesses.

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

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

Security Expertise

With 30 years of destruction expertise 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 one of thousands of small businesses, you can put the power of the largest shredding fleet and the largest service footprint in North America to work for you.

Customer Experience

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

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

About the 2020 Data Protection Report

Shred-it commissioned Ipsos to conduct a quantitative online survey of small business owners (SBOs) in the U.S. (n=1,000), with fewer than 100 employees and C-suite executives in the U.S. (n=100) with a minimum of 500 employees. Data for SBOs is weighted by region. Data for C-suites is unweighted as the population is unknown. The precision of Ipsos online surveys is calculated via a credibility interval. In this case, the U.S. SBO sample is considered accurate to within +/- 3.7 percentage points had all U.S. small business owners been surveyed, and the U.S. C-suite sample is accurate to within +/- 11.2 percentage points had all U.S. C-suite executives been surveyed. The fieldwork was conducted between February 27 and March 9, 2020.

In addition to the quantitative online survey, Ipsos conducted a short omnibus survey among a general population sample of n=2,011 Americans about data protection and security. The credibility interval for this sample group is +/- 2.5 percentage points, 19 times out of 20, of what the results would have been had all adults in the U.S. over the age of 18 been surveyed.

We protect what matters.

Shred-it®