Shred-it®

DATA PROTECTION REPORT 2019

U.S. ★ EDITION

Contents

Executive Summary 5

C-Suites vs. SBOs 7

Employees vs. Employers 14

Consumers 17

Industry Specific Insights 20

- Hospitality 21
- Legal & Finance 22
- Education & Healthcare 23
- Automotive 24
- Technology & IT 25

Ask the Expert 26

Conclusion 29

Foreword

On the global stage, America's business community has long been associated with disruption and innovation, but also operating with integrity, transparency and increasingly a commitment to being purpose-driven. At the core, it boils down to delivering on the evolving expectations of the American public.

In this vein, companies are quickly learning that prioritizing information security and safeguarding data in today's fast-paced, constantly-changing environment is critical. And while businesses, government and consumers alike acknowledge its importance, identifying gaps in data protection and determining what policies, procedures and actions need to be adopted requires a focused look at current and evolving risks and trends.

In thinking about recent drivers of data protection priorities, 2018 was dominated by the European General Data Protection Regulation (GDPR) and the implications of its compliance requirements to businesses and consumers around the world. California also became the first state to regulate online privacy with the introduction of the California Consumer Privacy Act (CCPA) – legislation focused on consumer rights, in particular the right to know what personal data is being collected, whether personal data is sold or disclosed and to whom, and the right to access the personal data being collected on an individual.

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

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

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

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

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

Executive Summary

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

Shred-it surveyed

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

The results are conclusive:

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

Policies are up, but policing is down. While 98% of C-Suites and 88% of SBOs indicated a strong understanding of legal requirements, only **73% of C-Suites acknowledge strict adherence to known and understood policies** for storing and disposing of confidential paper documents, and 69% confirm adherence to policies around end-of-life electronic devices. For **SBOs, 57% acknowledge strict adherence to such a policy** for paper documents, with only 42% confirming adherence to policies for end of-life electronic devices.

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

- **35% of Americans stated they would lose trust in an organization following a breach**
- **1 in 4 consumers would take their business elsewhere following a data breach**
- **Only a third believe that all digital data breaches are disclosed**
- **1 in 3 consumers say they would actively tell others about a breach to which they were victim**

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

The number of reported data breaches in the U.S. doubled in the past year:

43%

of C-Suites confirming a breach
(versus 32% in 2018)

8%

of small businesses reporting a breach
(up from 3% in 2018)

Despite this rise

55%

of C-Suite respondents support the statement that data breaches are

not a big deal
blown out of proportion

79%

of SBOs think any breach is

A BIG DEAL

86%

of American consumers agree with SBOs

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

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

- **47% of C-Suites and 31% of SBOs who reported a breach cited human error by employees/insiders as the main cause;**
- **Should a breach of employee data occur, 35% of employees indicated they are likely to seek work elsewhere.**

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

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

C-Suites vs. SBOs

U.S. businesses are in denial when it comes to data protection. Many leaders are unaware and unconcerned about the consequences of a material breach.

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

With seemingly endless news coverage of targeted consumer breaches by hackers, foreign cyber interference with elections, and social media privacy scandals, it is not hard to see why business leaders have been focusing data protection efforts on external threats. Unless immediate action is taken to address internal vulnerabilities, the human error and deliberate sabotage driving data breaches will impact U.S. businesses significantly.

The insights from this year's report show that business' understanding of the legal requirements related to handling confidential information is strong.

98%

of C-Suites indicated a strong understanding

88%

of SBOs indicating the same, up from 82% in 2018

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

» **Of greater concern? While 94% of C-Suites indicated that their organization had a known and understood policy** for storing and disposing confidential paper documents, and 90% for end-of-life electronic devices

» **Only 69% of SBOs indicated the same for paper documents, and 53% for policies around disposing of electronic devices.** While SBOs have made significant progress over the last year (up from 49% in 2018 for paper documents, and up from 34% in 2018 for electronic devices) there remains significant room for improvement.

Needless to say, an erosion of consumer trust and loyalty of that magnitude has the potential to significantly impact business operations, including the bottom line. **There is clearly an urgent need for organizations of all sizes to strengthen their policies, training and practices to safeguard the data entrusted to them by American consumers.**

2 in 10
would seek compensation or
take their business elsewhere (23%), and

1 in 3
would lose trust or
tell others about the breach (31%).

Here is why that matters.
Data from the 2019 DPR confirms that the evolving context of consumer sentiment across the U.S. is powerful.

Data Security and Consumer Trust

The results of this year's 2019 survey point to an underlying and significant theme of fragile consumer trust. From the 35% of Americans who indicated that they would lose trust in an organization following a data breach, to the finding that 66% of Americans do not believe that all digital data breaches are disclosed, the reputational impact of data protection cannot be understated.

While C-Suites and SBOs recognize data security risks, they underestimate consequences, creating a worrisome disconnect. Simply put, a data breach is a trust breach, and consumers will take their business elsewhere if they lose confidence in an organization.

America's business leaders need to take heed.

55%

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

86%

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

SBOs are a little more in tune with reality, as

79%

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

At the same time, the number of reported data breaches has increased over the past year, most significantly among SBOs.

43%

of C-Suites confirming a breach
(up from 32% in 2018)

among SBOs the number almost tripled to

8%

(up from 3% in 2018)

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

62%

of C-Suites and

28%

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

This year's DPR should be a severe wake-up call to America's business leaders. Those demonstrating a complacent attitude around the seriousness of data breaches risk taking a significant hit to their bottom line in addition to suffering reputational damage.

The Hidden Risks of Remote Work Policies

Businesses of all sizes are reporting a shift to more remote working, with

26%

of C-Suites indicating more than **76% of their workforce works away from the office on a regular basis, and**

17%

of SBOs indicating the same.

This year, the 2019 survey uncovered that both groups agree **flexible work arrangements are likely to become increasingly important to their employees over the next 5 years,** with

94%

of C-Suites agreeing
(up from 88% in 2018), and

79%

of SBOs agreeing
(up from 65% in 2018).

Last year's 2018 data uncovered that 80% of C-Suites and only 35% of SBOs had a policy in place for storing and disposing of confidential information at off-site locations. **This year, that number has risen – a full 91% of C-Suites confirmed such a policy is now in place, with 61% of SBOs confirming the same.** While that increase is promising, the numbers still indicate a significant blind spot for SBOs that needs to be addressed.

Leaders need to remain vigilant, monitor compliance and update policies as technologies and regulations evolve.

The Human Side of Data Protection

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

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

While deliberate sabotage and theft from both employees and vendors remain concerning, there was a significant increase among both C-Suites and SBOs citing human error or accidental loss on the part of an external vendor/source as responsible for a breach.

The number of **C-Suites citing external human error or accidental loss** as the cause, jumped to

53%

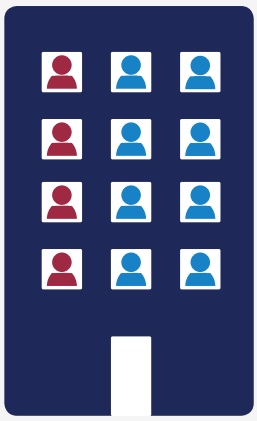
(up from 28% in 2018),

while the percentage of **SBOs citing external human error or accidental loss** jumped to

28%

from 17% in 2018.

Yet, while deliberate theft or sabotage by an employee/insider was a distant concern for C-Suites at 21%, SBOs appear to be more challenged by internal threats with 28% citing intentional actions on the part of employees as the cause for a breach.



The survey also uncovered an additional motive for priority to be placed on employees – an average of

33%

indicated they are likely to seek employment elsewhere following a data breach. Interestingly, 35% indicated they would seek employment elsewhere if the breach was related to employees' data, where a slightly lower 31% would seek employment elsewhere if the breach was related to customers' data.

The 2019 DPR reveals a clear misperception of the importance and impact of data security within businesses at all levels, while highlighting the significant potential insider threats facing U.S. businesses.

As leaders re-evaluate the effectiveness of their current policies, practices and awareness levels, shifting focus to the intentional and accidental threats presented by employees and external vendors/sources must take priority. The findings also offer a warning that leaders cannot ignore: consumers are starting to vote with their wallets. Lose their data and you may lose their business.

Thus, aside from ensuring policies are constantly updated and employees are trained on a regular basis on what is expected of them, businesses of all sizes must remain vigilant around insider threats, while championing the role employees and partners play in safeguarding the company's data.

Employees vs. Employers

The main cause of data breaches? Human error.

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

A Concerning Gap

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

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

88%

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

61%

feel their employees are

The gap is smaller for SBOs

54%

state they are very aware of such practices

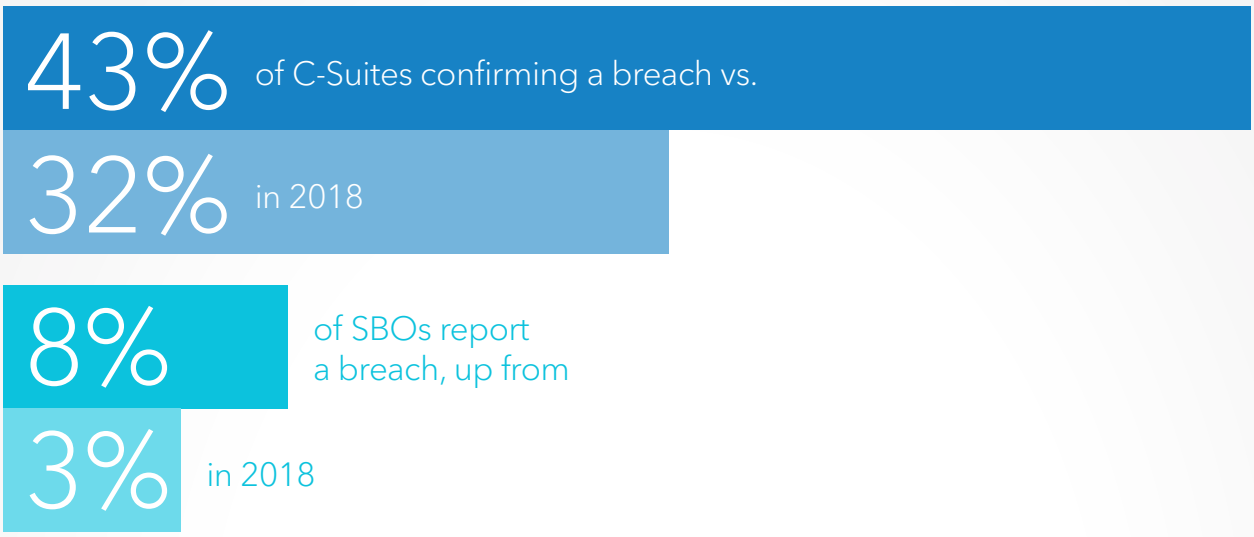
44%

feel their employees are

The different levels of awareness among all groups is surprising compared to the investment most large organizations claim they are making in training their employees on their data security protocol. Almost all U.S. C-Suites (98%) report that their business offers employee training – either once (10%) or on an ongoing basis (88%) – to help identify and prevent common cyber-attack tactics such as phishing, ransomware or other malware. In 2019, SBOs cited notably lower levels of training for employees at 68%. In short, there is a disconnect – particularly among C-Suite organizations – with weak data destruction practices not matching the training investment being made.

Beyond awareness of policies, employees and employers also view the threat of a breach quite differently. While the majority of American employees (58%) said they believe it is unlikely that their organization will suffer a data breach within the next 5 years, the reality is that the number of data beaches are on the rise.

Reported breaches in the U.S. increased significantly over the last year



Against this backdrop, a surprising number of Americans (29%) say they are unsure if their place of employment has ever suffered a data breach, with only 55% confidently able to say they have not.

Data Protection is Everyone's Responsibility

When asked who should take responsibility for data security within an organization, a majority of respondents (64%) indicated that it should be the employees, rather than management. This further highlights the need for effective and regular employee training.

Findings from the DPR reveal that many C-Suites (47%) and SBOs (39%) who view a data breach as being likely at their organization, within the next 5 years, expect human error by an employee(s)/insider(s) to be the cause.

The Human Capital Impact

Perhaps most alarmingly, this year's survey uncovered the potential human capital impact to organizations in the event of a breach. More than one-third of working Americans indicated they would likely seek new employment opportunities if their employer suffered a breach of customer (31%) or employee data (35%).

48%

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

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

	Millennials (aged 18-34)	Others (aged 35+)
Will go elsewhere if employee data is compromised	52%	25%
Would jump ship if customer data is compromised	47%	22%

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

Consumers

Consumers do not believe their personal data is safe.

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

One quarter (23%) of consumers surveyed indicated that they would take their business elsewhere following a data breach, which could be devastating for a business. Further, one in three consumers (31%) say that they would actively tell others about a breach to which they were victim, which highlights an urgent need for businesses to make information security a priority.

Indeed, their survival may depend on it.

An overwhelming

60%

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

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

Perception is Reality

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

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

86% **Consumers are nearly unanimous in their belief that any breach of their personal data is a "big deal"**

45% **In stark contrast, roughly half of leaders in America's largest corporations would put a breach in that same category.**

79% **The gap is much lower among SBOs, as more than three in four rate the impact of breaches as significant.**

While consumers feel less confident that their data is being safeguarded, the reality is that C-Suites and SBOs are in fact increasing their corporate policies, specifically when it comes to employees working off site or away from the office. **This year, 91% of C-Suites reported having a policy for disposing of confidential information when employees work away from the office, up from 80% in 2018, while the percentage of SBOs with such a policy increased to 61% up from 35% in 2018.** This disconnect needs to be resolved with demonstration to consumers that data protection is a corporate priority. This will ultimately help strengthen consumer confidence.

Rebuilding Consumer trust

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

Transparency has never been more important, especially with C-Suites. Almost one in two large businesses in the U.S. (43%) report having been breached – a level that is up significantly from 32% in 2018. Although SBOs are not as likely to be targeted, with only eight percent reporting a breach in 2019, they should implement the proper precautionary measures since smaller businesses may not be able to handle the financial and reputational consequences as easily. **Businesses need to walk the talk.**

1 in 3 Americans trust that digital data breaches are properly disclosed.

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

Ensuring consumers have visibility into and an understanding of those policies and practices is becoming just as important, as consumers' perception of how their data is – or is not – being protected, can be just as powerful as reality. By being consumer-centric and elevating the role of data security across an organization, businesses can strengthen consumer trust, corporate reputation and competitiveness.

23%

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

The good news is that 47% indicated they are willing to wait to see how an organization reacts to the situation before making their mind up about what to do, underscoring the importance of developing a recovery plan post breach.

Industry Specific Insights

Concerning trends across some of America's leading industries:
Increased Risk, Increased Denial and Decreased Trust.

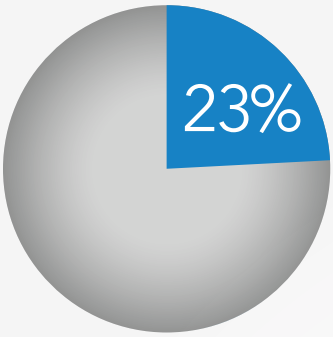
The 2019 DPR includes an in-depth look at industry-specific practices across hospitality, legal, financial services, education, healthcare, automotive and technology industries. **While business leaders in each sector face unique challenges and opportunities, the data revealed that risk, denial and trust are common themes** that can and should fundamentally shift how many U.S. businesses approach information security.

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

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

Hospitality

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



OF HOSPITALITY BUSINESSES dispose of paper documents they no longer need with locked consoles and professional shredding services.

Key 2019 DPR Findings

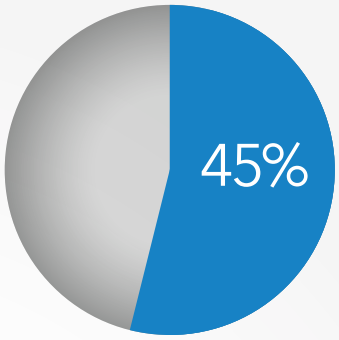
- While 31% of hospitality business leaders believe their customers will stop doing business with them if their organization were to suffer a data breach, 36% agree with the statement that breaches are "no big deal" and "blown out of proportion"
- 17% of hospitality industry respondents said they have a policy for storing and disposing of confidential information, but not all employees are aware of it
- A significant number of hospitality business leaders acknowledge that no data protection policies are in place at all, with 19% lacking a policy for disposing of paper documents, and 31% lacking a policy for disposing of information on end-of-life electronic devices
- 93% of hotel owners feel like they need to do more to show employees and consumers how they are protecting personal information

Legal & Finance

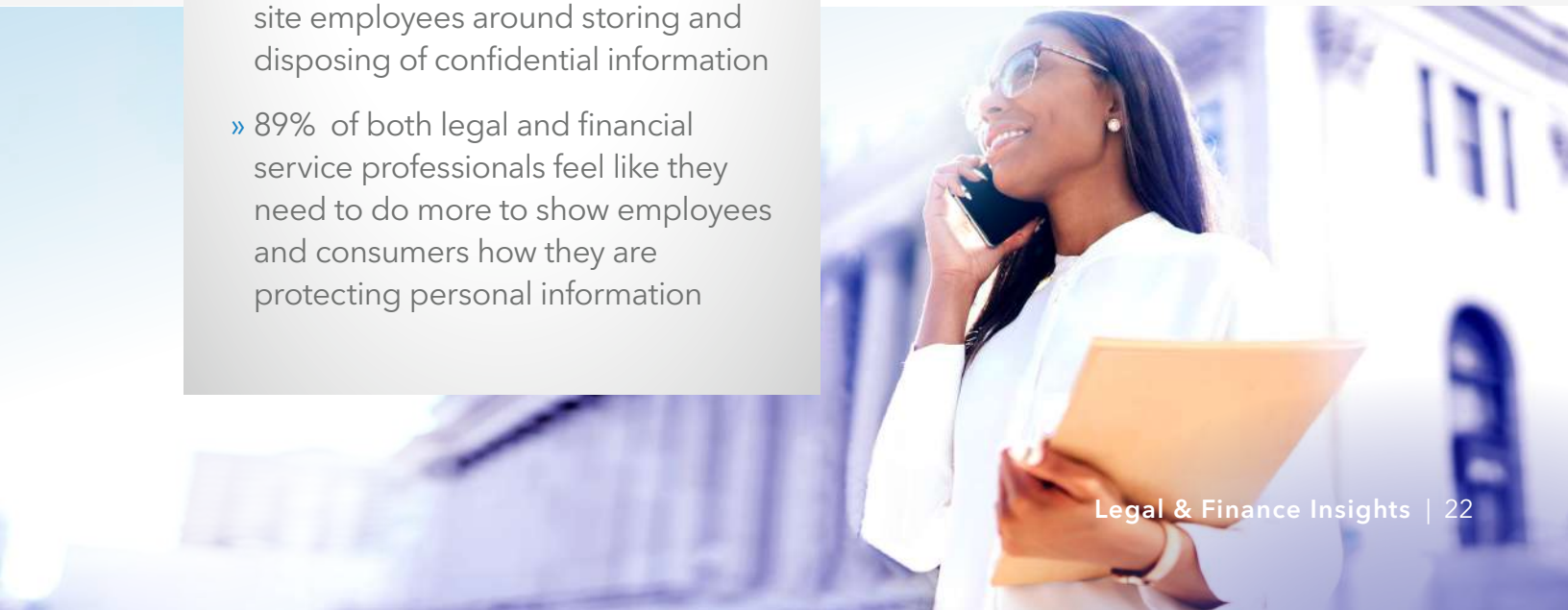
Lawyers, bankers and auditors make missteps, too. With the amount of confidential information collected, both law firms and financial services firms need to recognize that insufficient internal security protocols put their business at an increased risk. Human error – and not cybersecurity – is the leading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

Key 2019 DPR Findings

- 83% of consumers agree that digital data security is a top priority for them when choosing whom to do business with
- Only 15% of financial services and legal professionals confirm they have never trained employees on how to identify common cyber-attack tactics
- 77% of legal and financial service professionals agree that the risk of a data breach is higher when employees work off-site, yet 17% confirm that no policy exists for off-site employees around storing and disposing of confidential information
- 89% of both legal and financial service professionals feel like they need to do more to show employees and consumers how they are protecting personal information

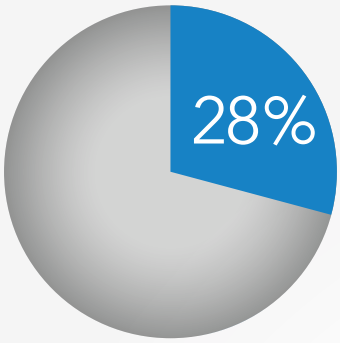


OF LEGAL AND FINANCIAL PROFESSIONALS acknowledge that human error or accidental loss by employees/insiders are likely the source of a breach.



Education & Healthcare

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



EDUCATION AND HEALTHCARE PROFESSIONALS use an in-office shredding machine but admit they do not use locked consoles for storing documents.

Key 2019 DPR Findings

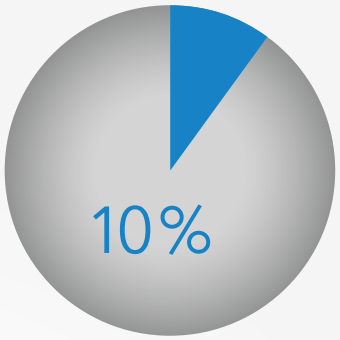
- 13% of education and healthcare organizations do not have a policy in place for storing and disposing of confidential paper documents, while 26% are without a policy for storing and disposing of confidential information on end-of-life electronics
- Only 5% of respondents recycle rather than shred confidential documents, while another five percent throw them in the garbage
- A full 18% of education and healthcare organizations do not have a policy specific to disposing of confidential information when working off-site/away from the office
- Education and healthcare professionals are almost unanimous (96%) in agreeing they need to do more to show employees and consumers how they are protecting personal information

Automotive

The majority of auto dealers realize that they are at risk. From credit card and driver's license information to details about their customers' financials, credit ratings and insurance, auto dealers are in possession of a significant amount of sensitive personal information, which makes prioritizing data protection a business imperative.

Key 2019 DPR Findings

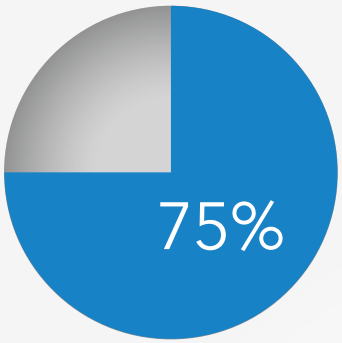
- 31% of auto dealers say they do not have a policy in place for storing and disposing of confidential paper documents, while 41% do not have a policy for disposing of confidential information on end-of-life electronics;
- While 71% of auto dealers believe the risk of a data breach is higher when employees work off-site than when they work in the office, nearly four in ten (39%) do not have a policy specific to storing and disposing of confidential information when working off-site;
- Nearly all (96%) auto dealers agree they need to do more to show employees and consumers how they are protecting personal information.



OF AUTO DEALERS are aware of the legal requirements for handling confidential information, but are not familiar with them.

Technology & IT

Technology and IT decision makers face unique data protection challenges and threats. The security of their own organizations' confidential information is a priority – and sometimes a challenge – for an industry with a significant portion of remote workers.



OF IT PROFESSIONALS have a strong understanding of legal requirements for handling confidential information.

Key 2019 DPR Findings

- 20% say no policy exists in their organization for storing and disposing of confidential paper documents, with 26% saying the same for information on end-of-life electronics;
- 75% of IT professionals agree that the risk of a data breach is higher when employees work remotely;
- 87% of IT professionals agree that the option to work remotely is going to become increasingly important to their employees over the next five years, yet 26% have no policy in place for storing and disposing of confidential information when employees work off-site/away from the office;
- While IT professionals are investing in digital security (61%), only 39% are investing in physical document security
- 94% of IT professionals feel like they need to do more to show employees and consumers how they are protecting personal information.

Ask the Expert

A Global Perspective on Data Protection and Security

Prepared by Ponemon Institute

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

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

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

Knowledge is the path to protection.

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

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

Predictions About Global Data Protection and Security.

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

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

The rise of nation-state attacks.

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

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

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

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

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

Cybersecurity governance practices are expected to improve.

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

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

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

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

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

Information security needs to be looked at holistically.

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

A Turning Point for American Business Leaders

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

Throughout the 2019 DPR, three prominent themes emerged:

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

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

American business leaders take note. Complacency will lead to breaches, and breaches will cost them – not just in reputation, but also in sales, profits, employee retention and more.

These threats are real, and regardless of the industry, all organizations must take action. Further, as businesses and modern workplace trends continue to evolve, data protection practices must evolve with them. The competitiveness of every business depends on it.

The good news is that there are tangible solutions that businesses can incorporate into their operations. Tougher information security and data protection policies, better training and ongoing policing are all part of the solution. So, too, is ensuring the entire organization knows what data to keep, what data to destroy, and how to do each without risk. Shred-it has the expertise and experience to be part of 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, an end-to-end secure chain of custody, our primary focus on document security ensures your confidential information remains confidential.

Service Reliability

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

Customer Experience

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

We protect what matters.

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

About the 2019 Data Protection Report

Shred-it commissioned Ipsos to conduct a quantitative online survey of Small Business Owners (SBOs) in the United States (n=1,000), with fewer than 100 employees and C-Suite Executives in the United States (n=100) with a minimum of 500 employees. Data for Small Business Owners is weighted by region. Data for C-Suite Executives is unweighted as the population is unknown. The precision of Ipsos online surveys is calculated via a credibility interval. In this case, the U.S. SBO sample is considered accurate to within +/- 3.5 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 US C-Suite Executives been surveyed. The fieldwork was conducted between March 26th and April 1st, 2019.

In addition to the quantitative online survey, Ipsos conducted a short omnibus survey among a gen pop sample of n=2,014 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.

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

Shred-it®