Shred-it®

2013 State of the Industry
Information Security

“Did you know? The majority of security breaches are error or malicious intent“

Contents

SECTION 1 | PAGE 4

INTRODUCTION

SECTION 2 | PAGE 5

SITUATION ANALYSIS

SECTION 3 | PAGE 7

INFOGRAPHICS

SECTION 4 | PAGE 9

PRODUCT FOCUS

SECTION 5 | PAGE 11

SUPPLY CHAIN

SECTION 6 | PAGE 12

TIPS

SECTION 7 | PAGE 14

INDUSTRY SPOTLIGHT

SECTION 1

INTRODUCTION

The 2013 State of the Industry Report shares insight and advice relating to areas of critical importance when it comes to securing sensitive information, including the disposal of obsolete electronic media, supply chain information security, staff training and organizational accountability.

In 2012, Shred-it released its inaugural State of the Industry Report, drawing attention to a range of information security issues that impact businesses of all sizes. The Report shared insights into the number of businesses not making information security a priority, how these businesses were affected and the steps businesses need to take in order to prevent information security breaches of this nature. The report also included enlightening statistics from the 2012 Shred-it Information Security Tracker program, a study commissioned to gain insight on information security policies and procedures among small businesses and C-suite executives in the United States and Canada.

This year's report builds on its predecessor and provides organizations across North America with tips and insights to help them safeguard their business against information security breaches. This edition of the State of the Industry Report shares key findings from the 2013 Shred-it Information Security Tracker survey to demonstrate what businesses of all sizes are doing, or not doing, to secure their data and protect their companies and their customers from the threat of a security breach, as well as business identity theft and fraud. The 2013 State of the Industry Report shares insight and advice relating to areas of critical importance when it comes to securing sensitive information, including the disposal of obsolete electronic media, supply chain information security, staff training and organizational accountability.

As there are so many areas to consider when it comes to information security, this report will help organizations better understand the need to take a 360-degree approach to information security policies and procedures.

SECTION 2

SITUATION ANALYSIS

Despite regular reports in the news of businesses being impacted by data breaches, organizations from across North America continue to be plagued by the loss of sensitive information.

It can be tempting for businesses to turn a blind eye to being proactive with their information security if they have never experienced fraud or a loss of data; however, the legal, financial and reputational repercussions can be devastating. When it comes to building a security strategy, there are some simple steps businesses can take to help avoid having their sensitive information fall into the wrong hands.

Safely and securely storing and destroying printed documents and any information stored on electronic media helps protect businesses from theft and data breaches that can cause serious financial and reputational damage. Businesses should make information security a priority because not doing so can lead to identity theft and fraud, which can result in financial impact, reputational damage, loss of customers, employee turnover and disengagement, and loss of competitive advantage.

The Shred-it 2013 Security Tracker provided detailed insight as to what businesses of all sizes are doing (or not doing) to protect their companies and customers from the threat of identity theft and fraud. The most surprising finding was that businesses of all sizes lack awareness about proper information security policies and procedures. Many American and Canadian businesses do not have known and/or understood information security protocols that are followed by all employees. Twenty-three per cent of small American businesses indicate they are either not at all or not very aware of their industry's legal requirements for storing or disposing of confidential data, in contrast to only one per cent of large American businesses being unaware of legal requirements. As well, 41 per cent of large American businesses state that they have security protocols in place, but not all employees are aware of these policies and procedures, while a striking 40 per cent of small American businesses admit that they do not have any protocols in place to protect confidential information.

As for Canadian companies, 22 per cent of small businesses indicate they are either not at all or not very aware of their industry's legal requirements for storing, keeping or disposing of confidential data, while 40 per cent of small Canadian businesses indicate they do not have any protocols currently in place. While only six per cent of large Canadian businesses do not have a known and understood protocol for storing and disposing of confidential data, 57 per cent of large

Canadian businesses do have protocols in place, but state that not all employees are aware of it. Only 35 per cent of large Canadian businesses indicate that employees are aware and adhere to the company protocol for storing and disposing of confidential data, while 46 per cent of small Canadian businesses report the same.

In addition to having established policies and procedures to keep sensitive information out of the wrong hands, many businesses across North America are not regularly training their staff, while some are not training staff at all. In the U.S., only 10 per cent of small businesses and 16 per cent of large businesses train staff on information security policies and procedures twice a year. One-third (34 per cent) of small American businesses admit that they never train their staff, while 40 per cent of small businesses train only on an as-needed basis. In Canada, only 24 per cent of large businesses train their staff twice a year, while only six per cent of small businesses employ training twice a year.

In an effort to ensure companies are making information security a priority, it is important to have someone responsible for managing data security issues, but many companies have not designated this responsibility. Since 2012, there has been an increase in the number of large American organizations reporting that they have no one responsible for managing data security issues (10 per cent in 2013, which is up from four per cent in 2012). Small American businesses remain consistent year-over-year, with 48 per cent of small businesses not designating someone to manage security issues in 2013 compared to 46 per cent in 2012. In Canada, the number of large businesses without someone responsible for managing data security issues has increased from six per cent in 2012 to 19 percent in 2013. Further, 45 per cent of small Canadian businesses admit that they do not have a person directly responsible for managing data security issues, which is a slight increase from 43 per cent in 2012.

Both American and Canadian businesses underestimate the potential impact of a data breach on their organization. The financial impact of those businesses that reported being victims of a breach appears to be on the rise, as 12 per cent of large American businesses and 15 per cent of large Canadian businesses experienced a breach resulting in a loss of more than $500,000.

"It is imperative that companies across North America remain vigilant when it comes to information security and take proactive steps to protect against data breaches."

A crucial first step for practicing effective information security is improving awareness of policies and procedures. Employees need to be made aware that data being lost or stolen can result in financial impact and harm to the credibility of an organization. The second step is the actual implementation of policies and procedures by enforcing sensitive data safeguarding as a company-wide practice.

As the way companies do business continues to evolve, the development and implementation of a proactive plan for safeguarding information becomes increasingly important. If businesses of all sizes want to remain competitive and profitable, they must safely and securely destroy documents and equipment to protect customers and employees. It is imperative that companies across North America remain vigilant when it comes to information security.

CANADA

WHERE IS THE GAP IN INFORMATION SECURITY?

PERCEPTION

55% OF CANADIAN BUSINESSES BELIEVE A SECURITY BREACH WOULD NOT SERIOUSLY IMPACT THEIR BUSINESS

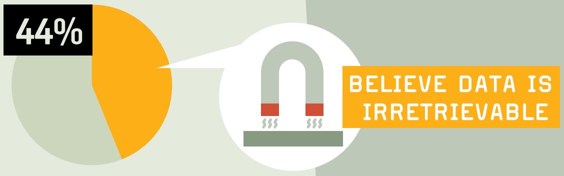
REALITY

THE AVERAGE COST OF A DATA BREACH IN 2012 WAS $5.4 MILLION*

22%

OF SMALL BUSINESSES

have little or no awareness of the legal requirements for storing or disposing of confidential data.



44% of Canadian companies both large and small mistakenly believe that wiping or degaussing a hard drive will make the data irretrievable.

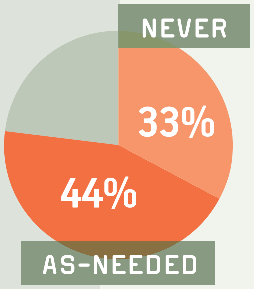
ONLY

6% & 24%

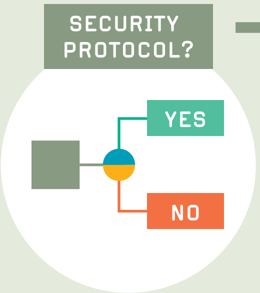
OF SMALL BUSINESSES

OF LARGE ONES

TRAIN STAFF TWICE A YEAR ON INFORMATION SECURITY POLICIES AND PROCEDURES.

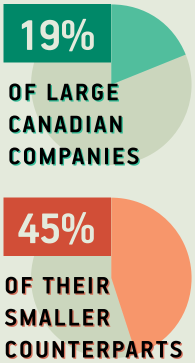


33% of small businesses never provide training, while another **44%** train only on an "as-needed" basis.



57% of large businesses have a security protocol **that isn't known by all their employees**.

40% of small businesses don't have any protocol at all.



have no one responsible for managing data security issues.

15%

OF LARGE BUSINESSES

who experienced a security breach indicated a loss of more than $500,000.

All of the statistics provided (unless otherwise stated) are from the Shred-it 2013 Information Security Tracker powered by Ipsos Reid

*2013 Cost of a Data Breach Study: Global Analysis." May 2013. www.symantec.com

USA

WHERE IS THE GAP IN INFORMATION SECURITY?

PERCEPTION

53% OF US BUSINESSES BELIEVE A SECURITY BREACH WOULD NOT SERIOUSLY IMPACT THEIR BUSINESS

REALITY

THE AVERAGE COST OF A DATA BREACH IN 2012 WAS $5.4 MILLION*

MORE THAN **1/3** OF SMALL BUSINESSES never train staff on their information security procedures.

SECURITY PROTOCOL? YES NO

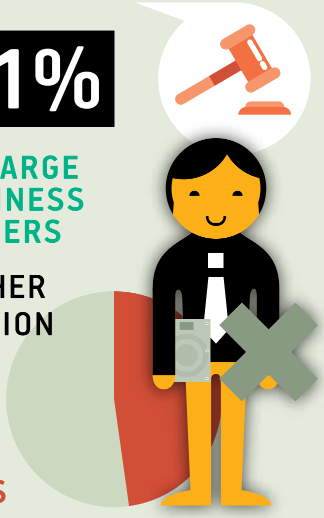
40% have no such protocols at all.

Over **12%** of C-suite executives have seen losses of more than $500,000 due to data breaches.

ONLY **18%** & **31%**

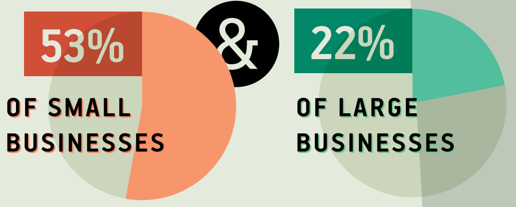
OF SMALL BUSINESS OWNERS & OF LARGE BUSINESS OWNERS

WOULD SUPPORT TOUGHER DATA PRIVACY LEGISLATION



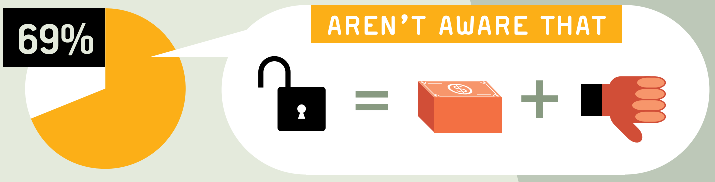
48% OF SMALL BUSINESSES have no one responsible for managing data security.

ONLY **16%** OF LARGE BUSINESSES TRAIN EMPLOYEES ON DATA SECURITY PROTOCOL TWICE A YEAR.



DO NOT SECURE THEIR CONFIDENTIAL MATERIAL BEFORE DESTROYING IT

69% of small business owners aren’t aware that lost or stolen data would cost them money and credibility.



All of the statistics provided (unless otherwise stated) are from the Shred-it 2013 Information Security Tracker powered by Ipsos Reid

*2013 Cost of a Data Breach Study: Global Analysis.” May 2013. www.symantec.com

SECTION 4

PRODUCT FOCUS

In an age that sees an increased risk of security breaches, it is of paramount importance that organizations protect their confidential information.

Though many businesses seemingly take the appropriate steps to protect themselves against data breaches, the proper protection of sensitive information continues to be a cause of concern.

Many businesses in North America, both large and small, are unaware of the implications of stockpiling old electronic media. Storing confidential information, in any form, puts organizations at risk of a security breach and liability. Often, companies will store items containing confidential information in a storage closet or at an offsite storage facility, underestimating the potential consequences of an information security breach related to these obsolete pieces of equipment.

Challenges in ensuring sensitive documents are kept private are not limited to paper-based documents. Shred-it's 2013 Information Security Tracker survey, which assessed the practices of small and large U.S. and Canadian businesses, demonstrated that only 22 per cent of C-suite businesses in the U.S. destroy their obsolete electronic devices, compared to 18 per cent of small businesses. In Canada, that number is even more alarming with only 18 per cent of large business fully destroying hard drive devices, compared to 14 per cent of small businesses.

Many Canadian businesses are unaware that the most effective way to prevent retrieval or recovery of this information is by fully destroying the device (60 per cent of large businesses compared to 42 per cent of small businesses in Canada). In the U.S., only 22 per cent of large companies completely crush and destroy hardware, while 18 per cent of small businesses do the same.

Overall, while large businesses seem to take information security more seriously than small businesses, as a whole, it has been found that businesses of all sizes mistakenly believe that wiping or degaussing a hard drive will render the data irretrievable, meaning that the majority of these companies inadvertently put themselves and their customers at risk of data being recovered.

Electronic media destruction is the most effective, secure way to permanently destroy data.

Shred-it's Electronic Media Destruction service:

- Fully destroys hard drives, memory sticks and photocopier memories rendering them completely useless and beyond repair
- The service offers peace of mind as it is the most effective way to ensure data cannot be recovered
- Allows businesses and IT professionals to track their information destruction history by issuing a Certificate of Destruction that lists all electronic media that has been destroyed along with individual serial numbers

> "Shred-it's 2013 Information Security Tracker survey, which assessed the practices of small and large U.S. and Canadian businesses, demonstrated that only 22 per cent of C-suite businesses in the U.S. destroy their obsolete electronic devices, compared to 18 per cent of small businesses."

What types of electronic media can be destroyed?

- Hard Drive (any kind of laptop, desktop, PATA, SATA and many more)
- Backup Magnetic Tapes (any kind of DLT, mini cartridges and many more)
- Floppy Disk (3.5 inch disk, 5.25 inch disks, and many more)
- Zip Disk (100 MB, 250 MB, and other large disks)
- Optical Media (CDs, DVDs, Blue Ray, and HD DVD)

Ultimately, improper destruction of confidential data could impact a company's bottom line, either through financial, reputational or client loss.

SECTION 5

ENSURE THE SUPPLY CHAIN MAKES INFORMATION SECURITY A PRIORITY

It is of crucial importance to ensure everyone in an organization is aware of policies and procedures pertaining to information security.

At the same time, it is equally important to ensure awareness is top-of-mind among an organization's supply chain. Businesses large and small may be leaving themselves, their clients or their customers at risk if their business partners or members of their supply chain do not have similar information security procedures or protocols.

It is necessary for organizations to take proactive steps to protect sensitive information.

Below are some questions companies of all sizes should ask themselves when it comes to ensuring members of the supply chain are adhering to similar guidelines when it comes to information security:

- Do partners within the supply chain demonstrate a commitment to information security?
- Are supply chain partners aware of their industry's legal requirements when it comes to information security?
- Are potential business partners meeting contractual security requirements?
- What procedures are in place to properly maintain information security?
- Are there information security policies in place and do they align with your company's policies?

SECTION 6

TIPS FOR SMALL AND LARGE BUSINESSES

TIP

Why do I need to have an information destruction process in place?

Information security remains a key component of all privacy legislation and compliance standards in North America. As such, it’s not just good business practice to keep your confidential materials protected – it’s the law. The printing of documents is still standard practice in most workplaces. Unless confidential printed documents are disposed of securely, there is always the risk that they could fall into the wrong hands, threatening the security and privacy of your business.

Chain of custody and duty of care.

All businesses have a duty of care to their employees and customers to ensure that information is both kept secure and disposed of in a compliant manner. You should receive certification that the documents have been destroyed by your data destruction handler, which also means businesses can prove they have fulfilled their obligations.

Create a culture of security.

Businesses of all sizes lack awareness about breaches and proper information security policies and procedures. To safeguard sensitive data, it is critical to implement company-wide training programs to help avoid financial repercussions and/or reputational damage. Staff should understand why information security is important and be regularly trained on the most recent protocols and regulations concerning the safe and effective destruction of confidential information.

To become less susceptible to potential data loss and security breaches, conduct regular security audits to assess security performance and appoint a staff member to ensure that proper policies are in place.

Don’t overlook electronic media.

When upgrading computer systems, businesses may choose to utilize free data destruction software that erases, reformats, overwrites or degausses information stored on hard drives. These options are not completely secure as the actual data remains. The only way to completely protect your information is through permanent professional hard drive destruction of equipment.

TIP

Make information security convenient.

All companies should make information security convenient for employees by having a locked receptacle in the office or at easily reachable locations to ensure that no one has access to sensitive documents or electronic media after they have been disposed of.

Businesses of all sizes should place secure containers in permanent locations so that employees can drop off confidential documents without worrying about others gaining access to private information. Confidential information must be destroyed once it is no longer needed or the legal retention period is met.

Analyze possible security gaps within the organization.

Both small and large businesses are operating in increasingly expansive supply chains, and are often outsourcing services to various vendors and sharing sensitive information to facilitate business transactions. By creating far-reaching information security policies that encompass business partners and suppliers, companies can do a more effective job of protecting confidential data.

Work with security experts to assess existing security systems and ensure that all business partners demonstrate a commitment to information security and are following similar policies and procedures with regard to properly destroying information.

Implement a "shred-all" policy.

To avoid the risk of human error or poor judgment, don't ask your employees to decide what information is confidential. Implement a "shred-all" policy to remove the decision making process of what documents are confidential and what aren't, ensuring all documents that are no longer needed are promptly and properly destroyed.

Think prevention, not reaction.

Instead of just dealing with breaches as they happen, businesses of all sizes should implement ongoing risk analysis processes and create a policy specifically designed to limit exposure to fraud and data breaches. Reach out to an information security company for a free risk assessment that will help determine areas of improvement to protect against the impact of a data security breach.

Assign Responsibility.

Select an employee(s) to conduct periodic checks to identify potential security issues, and have this employee complete tasks such as ensuring security programs are regularly updated on all computers, request employees periodically change passwords, conduct employee trainings and flag potential information security gaps to all staff. In addition, work with a third-party professional vendor to develop a strategic approach to ensure the secure and safe destruction of all unneeded documents.

SECTION 7

INDUSTRY SPOTLIGHT

Both large and small businesses are equally at risk of a security breach, but for varying reasons. Large businesses are faced with a variety of issues such as managing more people, in more locations, which creates a higher likelihood of security breaches. Large businesses also operate in increasingly expanding and far-reaching supply chains and, as a result, share sensitive information with more and more vendors, thereby creating more opportunities for breaches. In addition, because of their size, large businesses may be slower to adapt to any suggested policies and procedures, as opposed to small businesses that are more nimble and have the ability to adapt more quickly to change.

Small businesses, however, may be more budget-conscious than large businesses, resulting in an inability to pay for third-party assistance with information destruction. Employees at small businesses may also believe that because of their size, they are at less risk of a security breach, resulting in a more relaxed attitude toward the protection of sensitive information.

While large and small businesses may face different security threats, the result of not having policies and protocols in place is the same. Businesses must make document security a priority because not doing so can lead to a variety of issues such as identity theft and fraud, propriety information getting into the wrong hands, loss of customers, employee turnover, disengagement and loss of competitive advantage. A breach can be incredibly expensive to the organization, as the investigation takes resources away from core business operations and any publicity surrounding the breach can result in long-term financial and reputational damage. In addition, companies without policies and protocols in place are at an increased risk of not being in compliance with a variety of federal and state or provincial privacy regulations, which could potentially result in significant fines.

Once businesses identify the importance of having security protocols in place, they must decide as an organization how to address these issues. First and foremost, businesses must receive executive approval and buy-in regarding the importance of information protection, which then needs to be communicated to all employees and contract staff. Organizations should conduct an internal risk assessment to determine weaknesses, but should also reach out to reputable third-party organizations, such as Shred-it, to identify vulnerabilities. Once a policy has been developed, an organization must educate employees – not just once, but provide continuing education to reinforce the importance of policies and procedures – and begin the process of implementation. Finally, businesses of all sizes must remain vigilant with regard to information security policies and continue to monitor and update protocols as necessary.

Document destruction companies can play an integral role in the development of policies and protocols for businesses of all sizes and can help organizations implement these procedures to protect themselves from a security breach. A crucial first step for practicing effective information security is improving awareness of policies and procedures. Employees need to be made aware that data being lost or stolen can result in financial impact and harm to the credibility of an organization. The second step is the actual implementation of policies and procedures by enforcing sensitive data safeguarding as a company-wide practice.

Hiring a reliable third-party professional vendor to help companies develop a strategic approach to ensuring compliance with legal requirements and the secure and safe destruction of all unneeded documents is recommended. A professional can assist in both the development and implementation of security protocols and recommend that any solution be based on a holistic, integrated perspective on security across an organization. Companies should identify all potential risks that may threaten the security of the organization's confidential information, including customer, business and employee-related information.

Considerations to make when developing policies and procedures include the following:

- **Implement a 'shred all' policy.** One of the most effective ways to prevent security breaches from either inside or outside an organization is by implementing a 'shred all' policy. A 'shred all' policy ensures that all documents are fully and securely destroyed on a regular basis. Rather than 'disposing' or 'discarding' of confidential data that is no longer needed, employees should be trained in the values of 'destruction at the source'.

- **Electronic Media destruction.** Ensure any electronic data storage devices, such as hard drives or photocopier memories, are physically destroyed when no longer needed. Simply erasing, wiping or degaussing drives does not mean that the data cannot be retrieved. Physical destruction is the only way to render electronic storage completely useless.

- **Consider supply chains.** In addition to internal policies and procedures, both small and large companies should ensure that partners or members of their supply chain are making information security a priority. Companies should ask themselves if their partners and suppliers demonstrate a similar commitment to information security.

- **Other potential protocols could include:** restricting access to confidential data based on specific business needs of personnel; training staff in secure document management and destruction; and providing employees with a locked console where they can deposit unneeded documents prior to disposal.

As the way companies do business continues to evolve, the development and implementation of a proactive plan for safeguarding information becomes increasingly important. If businesses of all sizes want to remain competitive and profitable, they must safely and securely destroy documents and equipment to protect customers and employees. It is imperative that companies in North America remain vigilant when it comes to information security.

Shred-it is a world-leading information destruction company providing document destruction services that ensure the security and integrity of our clients' private information. The company operates 140 service locations in 16 countries worldwide, servicing more than 150,000 global, national and local businesses, including the world's top intelligence and security agencies, more than 500 police forces, 1,500 hospitals, 8,500 bank branches and 1,200 universities and colleges.

shredit.com

1-888-750-6450

Shred-it®