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

INTRODUCTION

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 included enlightening statistics from the 2012 Shred-it Information Security Tracker programme, a study commissioned to gain insight on information security policies and procedures among small and large businesses in the UK. It highlighted case studies for information security breaches, shared tips for best practices, examined changes in privacy legislation and looked ahead at possible information security challenges and threats to businesses in the future.

This year's report builds on its predecessor and provides UK organisations 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 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 organisational accountability. As there are so many areas to consider when it comes to information security, this report will help organisations better understand the need to take a 360-degree approach to information security, policies and procedures.

SECTION 2

SITUATION ANALYSIS

Despite the increasing risk of suffering a data breach, UK businesses continue to lack awareness of the damage caused when sensitive information is lost or stolen.

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 UK businesses lack understanding of basic information security protocols that should be implemented and followed by all employees.

Only 40 per cent of small business owners and 70 per cent of senior executives in larger firms are aware that a data breach could result in severe financial impact and harm the credibility of the business. Small and medium sized businesses (SMEs) in particular still do not believe that a data breach would have a material impact on their business. This leads to them being 10 times less likely to have an information security system set up than is the case with larger businesses.

The vast majority of UK businesses both large and small are generally not aware of the many costs that may be associated with a data breach. Most seemingly believe that a data breach is a one-off affair with few, if any, long-term consequences. As well, 45 per cent of large businesses state that they have security protocols in place, but not all employees are aware of these policies and procedures, while a striking 42 per cent of small businesses admit that they do not have any protocols in place to protect confidential information.

In addition to having established policies and procedures to keep sensitive information out of the wrong hands, many businesses across the UK are not regularly training their staff, while some are not training staff at all.

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. Seventy seven per cent of larger businesses have an employee directly responsible for managing information security issues at management level (66 per cent) or board level (11 per cent) compared with less than half of SMEs (48 per cent). Furthermore, 95 per cent of large businesses have an employee devoted to data protection compared with only 53 per cent of small business owners, suggesting that larger businesses better understand the potential threat of data breaches and have put control systems in place accordingly.

UK businesses are underestimating the potential impact of a data breach on their organisation. The financial impact of those businesses that reported being victims of a breach appears to be on the rise, as 1 per cent of small businesses and 15 per cent of large businesses experienced a breach resulting in a loss of more than £300,000.

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 organisation.

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 supplier 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. Shred-it can assist in both the development and implementation of security protocols and suggests that any solution be based on a holistic, integrated perspective on document security throughout the document lifecycle across an organisation. Companies should identify all potential risks that may threaten the security of the organisation's confidential information, including customer, business and employee-related documents. Documents should be protected from the moment they are created until the time they are no longer needed.

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 UK companies remain vigilant when it comes to information security.

UK

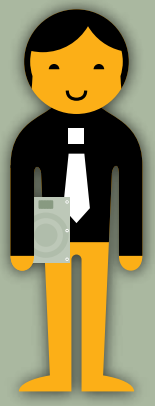
WHERE IS THE GAP IN INFORMATION SECURITY?

PERCEPTION

58% OF UK BUSINESSES BELIEVE A SECURITY BREACH WOULD NOT SERIOUSLY IMPACT THEIR BUSINESS

REALITY

THE AVERAGE COST OF A DATA BREACH IN 2012 WAS £2.1 MILLION*

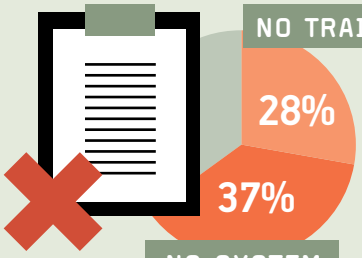


77% OF LARGE COMPANIES

VS

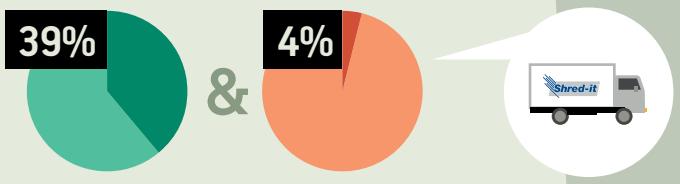
ONLY **48%** OF SMALL ONES

have someone responsible for information security issues at management or board level.



28% of UK small businesses have never provided training on information security to employees.

37% don't even have a protocol for managing information security.

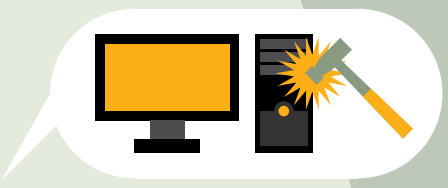


ONLY 39% OF LARGE BUSINESSES AND 4% OF SMALL ONES USE A PROFESSIONAL SHREDDING SERVICE TO DISPOSE OF SENSITIVE DOCUMENTS. COMPANIES WITH REVENUE OVER £1M ARE 8 TIMES MORE LIKELY TO DO SO.

2 OUT OF EVERY **5** LARGE BUSINESSES

prosecuted for a data breach reported a loss of more than £500,000.

COMPARED TO LARGE BUSINESSES, SMALL ONES ARE LESS THAN HALF AS LIKELY TO BE AWARE OF THE EU DATA PROTECTION DIRECTIVE REFORMS.



LESS THAN **1/4** OF BUSINESSES both large and small crush their electronic media.

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 organisations protect their confidential information.

Though many businesses are seemingly taking 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 the UK, both large and small, are unaware of the implications of stockpiling old hard drives. Storing confidential information, in any form, puts organisations at risk of a security breach and liability. Often, companies will store items containing confidential information in a store cupboard 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 UK businesses, demonstrated that only 46 per cent of C-suite businesses wipe their obsolete electronic devices, compared to 62 per cent of small businesses.

Many UK businesses are unaware that the most effective way to prevent retrieval or recovery of this information is by fully destroying the device. In the UK, only 26 per cent of large companies completely crush and destroy hardware, while 24 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.

Hard drive destruction is the most effective, secure way to permanently destroy data. Shred-it's Hard Drive 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

"Only 23% of large and 25% of small businesses crush their electronic media – which means the vast majority of UK businesses are inadvertently putting themselves and their customers at risk."

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 organisation is aware of information security policies.

At the same time, it is equally important to ensure awareness is a priority among an organisation'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 organisations 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

BUSINESS GUIDE TO SECURE DESTRUCTION

TIP

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

Information security remains a key component of all data protection legislation and compliance standards in the UK. 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.

What information do I need to destroy?

There are four main categories business information falls into; confidential, business confidential, sensitive or personal information. This includes documents with signatures, bank account numbers, medical, legal and credit information. Businesses also need to consider how they destroy their intellectual property. Throwing away new product reports, training information, performance reviews, financial results or marketing strategies is just as harmful to your business.

A 'shred all' policy is therefore the perfect solution because it eliminates any confusion and also helps create a consistent secure information destruction management standard. Your employees don't have to decide what to shred. They simply shred all business documents keeping your customers, employees' and business information secure. Shred-it also recycles all the paper they shred so you are able to combine two different waste streams and save money.

Is the shredding process itself secure?

Businesses need to ensure that any containers provided by their information destruction supplier are lockable and secure. Once documents have been placed inside the containers, they should not be retrievable. Shred-it provides secure consoles for this purpose.

TIP

Have you identified your risk areas?

A security risk assessment helps to determine the level of information security in your business and that helps identify risks and how to put a secure and safe information destruction programme in place.

Shred-it offers a free risk assessment service by a trained and background checked representative. An online risk assessment survey is also available on the website. This will help you to determine how you are managing confidential information and the information destruction process.

On site or off site shredding?

Document shredding on or off site should be done inside a locked area that is not accessible to anyone but the document destruction handler. Documents should never be sorted before destruction and the most secure shredding method is one that you can witness actually at your location. A professional cross-cut shredding machine should be used and there should be regular scheduled collection and disposal of your documents.

How do you stay secure when working from home?

Treat your home working space as you would your office or workplace. Take your documents back to work in a secure manner and destroy any documents there when possible. Assume that all business documents are confidential and only take them out of the work place if it is absolutely necessary. Do not print off any confidential information from laptops or computers unless absolutely necessary.

What about information stored on digital devices?

Making sure you destroy products such as hard drives, USB sticks and other electronic and media related goods is important.

What happens if I fail to be compliant?

All UK organisations must comply with the Data Protection Act (DPA). If your organisation is found to be in breach of the DPA you could be subject to a penalty from the UK Information Commissioner's Office (ICO) of up to £500,000. But it's not just the cost of a security breach that you need to consider. The biggest cost comes in the form of irreparable damage to your business' reputation – something that has taken years to build.

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 suppliers, 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 flexible 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 document and equipment 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 organisation, 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 procedures in place are at an increased risk of non-compliance with a variety of data protection and information security regulations, which could potentially result in significant fines.

Once businesses identify the importance of having security protocols in place, they must decide as an organisation 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. Organisations should conduct an internal risk assessment to determine weaknesses, but should also engage reputable third-party organisations, such as Shred-it, to identify vulnerabilities. Once a policy has been developed, an organisation 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 organisations 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 organisation. 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 supplier 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. Shredding companies can assist in both the development and implementation of security protocols and recommend that any solution be based on a holistic, integrated perspective on document security throughout the document lifecycle across an organisation. Companies should identify all potential risks that may threaten the security of the organisation's confidential information, including customer, business and employee-related documents. Documents should be protected from the moment they are created until the time they are no longer needed.

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 organisation 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'.

- **Hard drive 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 the UK 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.co.uk

0800 197 1164