State of the Industry

Information Security

2016 GLOBAL

Shred-it®

Table of Contents

Introduction

The Global edition of Shred-it's State of the Industry Report is designed to provide organizations both large and small with actionable intelligence on the global technology, business, and policy trends that are impacting information security.

Introduction

The report draws on the detailed findings from the annual Shred-it Information *Security Tracker*, an in-depth targeted research study conducted on behalf of Shred-it by Ipsos.

The *Security Tracker* study provides global insights on information security policies and procedures among Small Business Owners (SBO) and C-Suite Executives (C-Suites) across the globe. This data offers a unique international outlook and provides insights on emerging risks and highlights how different geographies are prioritizing data protection and information security.

The Global edition of the 2016 State of the Industry Report reveals a number of common themes and emerging challenges that businesses are facing. These include:

Growing Awareness: Governments around the world are enacting stringent regulations in relation to information security. While there is a steadily growing awareness among C-Suites and SBOs with respect to these legal requirements of storing and disposing of confidential data, some countries continue to face confusion around legislative requirements and face a need for the Government to offer clearer guidance around organizational responsibilities.

Flexible Workplaces: Business culture around the world is changing. Increasingly flexible workplaces with growing numbers of remote and mobile workers may pose a significant information security risk for businesses in the future. An organization's ability to effectively manage the tools of the modern remote and global workforce – including USBs, laptops and mobile devices – will help determine the overall success of their approach to information security.

Ongoing Training: Workforce training to familiarize employees with policies and procedures related to information security can help mitigate the risk of human error and keep information security a priority. Frequent training and an employee ambassador program may be keys to training effectiveness.

Hardware Management: Instituting strong protocols and policies that govern how legacy electronic hardware is stored is critical to an organization's approach to information security management. The global research reveals that many larger organizations are thinking beyond storage and are destroying legacy equipment and devices more often. Among them, the leading organizations are leveraging third party expertise to regularly destroy hardware.

In addition to the themes and emerging challenges identified above, the study also found that risks of financial loss as a result of a data breach continues to be well understood by both of the groups surveyed. This is supported by the recent results of IBM and Ponemon Institute's 2016 Cost of Data Breach Study which found that the average total cost of a data breach has increased by 29% since 2013[1].

Also understood are the intangible aspects including customer trust, organizational reputation and sustainability. Trust and reputation are universal and considered to be among the most valuable of corporate assets and must be protected accordingly.

To ensure that their information security policies keep-pace, C-Suites and SBOs alike should be taking a broader view of information risks and impacts. The Global edition of the Shred-it 2016 State of the Industry Report provides a starting point.

[1] 2016 Ponemon Cost of a Data Breach, Page 1

Situation Analysis

GLOBAL

Globally, business leaders recognize the growing importance of data security in their organizations. With fewer borders and more mobility among employees, businesses need to bridge the gap between awareness and action to help give employees the training and tools they need to protect confidential information.

Impact of Data Breach

Just how seriously are companies taking the threat of a data breach? While companies appear to understand that data breaches are a real possibility, many are still of the mindset that the loss of confidential data won't have a significant impact on their organization's ability to operate. According to the Shred-it 2016 *Security Tracker* survey, only slightly more than half (52%) of global respondents feel that lost or stolen data would have a significant impact on their business. More surprisingly, only a quarter (24%) of those that perceived an impact from a breach, felt the greatest damage would be to the company's credibility or reputation, with legal and financial impacts being selected second and third, respectively. However, as noted by the Ponemon Institute's 2016 Cost of Data Breach Study, damage to a company's reputation can quickly lead to financial damage[2]. Following a data breach, management needs to take steps to retain customers' trust in order to minimize the financial impact of lost business.

Source of Data Breach

Globally, companies are becoming aware that the actions of their employees can place their confidential data at risk. Our research reveals that 45% of global respondents believe human error or accidental loss by an employee or company insider is the most likely source of a data breach.

Despite this perception, the majority of businesses are not implementing protocols required to help employees keep customer and competitive information secure. Almost half (40%) of global businesses leaders have no employee guidelines for storing and disposing of confidential information when working off-site or from home. This lack

[2] 2016 Ponemon Cost of a Data Breach, Page 1

of protection is even more concerning when you consider that the Ponemon study found that most data breaches (48% in this year's study) continue to be caused by criminal and malicious attacks and that a quarter (25%) were a result of human error[3].

By failing to ensure employees understand and follow security policies, businesses may be putting their organization and reputations at risk by exposing valuable customer, employee and business data to both internal risks like human error and external risks like malicious attacks or hackers.

But organizations are not only examining the risks they face today, they are looking to the future. With employees becoming more mobile and the increasing dependence on remote access, it is not surprising that 35% of global respondents feel that the leading security threat to their organization in five to ten years will be online with the next two greatest concerns being lack of internal knowledge or human error as a result of insufficient knowledge (16%) and cloud computing (14%). Organizations must not only acknowledge the emerging information security risks associated with a changing workplace, but they must ensure their policies and proceeds evolve to address these potential sources of a data breach.

Most Significant Type of Document Breached

When companies start looking at the various ways in which data may be breached, it seems as though the threat becomes more real. In fact, when asked about the impact of various types of documents, a majority of global businesses surveyed (71%) recognize that stolen documents or data could impact the stability of their company. In every country, client and customer information was chosen by the most number of companies (40% globally) as having the greatest risk if breached, while financial records were chosen as the next greatest risk (29% globally).

[3] Ponemon 2016 Cost of a Data Breach Study, Page 2

Security Tracker Infographic (GLOBAL)

THE IMPORTANCE OF DATA SECURITY

GLOBALLY, BUSINESS LEADERS HAVE BEGUN TO RECOGNIZE THE IMPACT OF A DATA BREACH

Personal Decryption Leak Backdoor
Confidential Crime Internet Theft Network
Information Identity Sensitive
DATA Incursion Confidential
Stolen BREACH Hacking
Security Batch Technology
Intentional Threat Payment Business Hackers Transaction

IF DATA WERE LOST OR STOLEN:

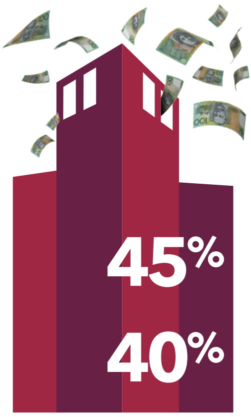
52% would significantly impact thier organization

24% damage credibility and reputation

14% cause financial harm

13% there would be legal consequences

BUT BUSINESSES ARE NOT PROVIDING THE TRAINING OR TOOLS TO HELP EMPLOYEES KEEP CUSTOMER & COMPETITIVE INFORMATION SECURE



45% believe human error or accidental loss by an employee or company insider is the most likely source of a data breach

40% have no employee guidelines for storing and disposing of confidential information when working off-site or from home

NEXT 5-10 YEARS

organizations see these as the biggest risks:

ONLINE THREAT 35%

HUMAN ERROR 16%

Resulting from Insufficient Knowledge

CLOUD COMPUTING 14%

BUSINESSES MUST CREATE INFORMATION SECURITY ACTION PLANS

to help employees protect confidential information.

For more information on protecting your workplace, visit shredit.com

All statistics from Shred-it 2016 Information Security Tracker powered by Ipsos

Shred-it®

Best Practices for Workplace Information Security

Information security threats are widespread and occur on a daily (if not hourly) basis. Unless organizations take steps to properly protect customer, business and employee information, they are vulnerable to these risks and can inadvertently open the door to information loss, identity theft, security breaches, and even criminal fraud.

Best Practices for Workplace Information Security

Implementing an information security plan to protect data is vital in managing these information security threats, and a step companies of all sizes around the world should take to mitigate the risk of a data breach.

Shred-it has identified 10 information security best practices that all businesses, regardless of size, geography and resources, can put in place to protect their customers, their reputation, and their people:

Lead from the top: When management demonstrates a commitment to information security, employees are more likely to follow suit. If managers behave in a way that undermines security policies and procedures, employees won't take them seriously either. No one is above the law.

Educate Employees: Employees need regular training to understand their organization's information security policies, spanning online, electronically-stored and physical information to ensure they are aware of how to handle and dispose of confidential information. A well-trained workforce is essential to protecting your organisation from a potentially damaging data breach.

Resist complacency: As organizations change and grow, so do their information security risks. It is important to regularly revisit security policies and procedures to ensure they reflect the realities of a constantly changing business

Implement a *Shred-it All* Policy: A *Shred-it All* policy removes any uncertainty around whether documents are confidential by requiring all paper documents to be shredded before being recycled or disposed. This simple step is one of the easiest ways to avoid human error including mishandling of confidential documents and files. In addition, all shredded paper is recycled, adding an environmental benefit to a security solution for businesses.

Institute a Clean Desk Policy: A Clean Desk policy encourages employees to clear their desks and lock documents in a filing cabinet or storage unit when they step away from their workstation for an extended period and at the end of each work day. This includes documents, files, notes, business cards, and removable digital media like memory sticks. Unattended and untidy work stations pose a greater risk as loose information is an easy target for theft.

Create a retention policy: Determine which documents you must keep and for how long. Clearly mark a destruction date on all records in storage and remember that the retention of some documents for a minimum period of time may be a legal requirement in itself. As part of the policy, organizations should also perform regular clear ups of storage facilities and avoid stockpiling unused hard drives

Protect Collaborative Spaces: A collaborative workplace can result in increased productivity and innovative thinking. However, confidential information left on whiteboards, note pads or flip charts can increase an organization's security risks as the information is available in common areas for any passerby to see. Collaborative spaces should be cleared once used. Employees can take a photo of whiteboards or flip charts and save them to a secure server for future use.

Encrypt All Electronic Devices: Encrypt all electronic devices used by employees regardless of whether employees use their own devices or devices provided through the company. In the event that electronic devices are lost or stolen, encryption will protect the confidential information stored on the device and mitigate any compromising activity.

Protect Printing Stations: Encourage employees and staff to not leave documents unattended at a shared printing station. To strengthen security around printing stations, consider using passwords for printing jobs.

Limit access: Set permission levels on who can access certain types of confidential information. Only authorised personnel should handle confidential information.

In addition to these tips, businesses should endeavor to stay up to date on current information security laws and the legislation that impacts them while ensuring their own information security policies and procedures comply with the government's policies. If found noncompliant, business can incur significant fines and face serious consequences.

Be Future Ready: Preparing for the Mobile Worker Challenge

Globalization of the business environment has driven the growth of the mobile worker as the new face of the future workforce. In fact, recent studies estimate the global mobile workforce is expected to increase to 1.75 billion by 2020 and account for 42% of the global workforce[4].

[4] https://www.strategyanalytics.com/access-services/enterprise/mobile-workforce/market-data/report-detail/global-mobile-workforce-forecast-2015-2020#.V2rYofkrKUk

Be Future Ready: Preparing for the Mobile Worker Challenge

In addition to giving organizations access to a larger pool of talent from which to hire, a mobile workforce offers several benefits to both employees and organizations including increased flexibility for employees and lower overhead and administrative costs for organizations.

For the global mobile workforce, technology is both the key enabler and driver for growth. Increasingly affordable smartphones and tablets combined with the growing acceptance of corporate bring your own device (BYOD) programs are making it easier than ever for employees to do their jobs remotely. According to International Data Corporation (IDC), mobility has become synonymous with productivity both inside and outside the workplace and the mass adoption of mobile technology has created an environment where workers expect to leverage mobile technology at work[5].

However, many organizations may not be prepared for the information security challenges that come with managing a mobile workforce. Shred-it's 2016 *Security Tracker* study reveals a shocking 40% of organizations do not have an information security policy in place that addresses off-site and flexible work environments and only 31% have a policy in place that addresses both. This demonstrates that the majority of businesses are not providing their employees with the protocols and training required to help them keep customer and competitive information secure in a mobile environment.

To help manage the increased risk of a mobile workforce, businesses of all sizes should be proactive in introducing training to keep employee, customer and company data safe and ultimately avoid information security breaches.

Here are 6 tips to help organizations manage information security for a mobile workforce:

1. Training for Mobile Workers: It can be challenging for an organization to ensure that mobile workers are disposing of confidential information in a safe way. Encourage proper practices through training that specifically highlights policies for remote workers. Ensure that obsolete mobile devices are properly disposed of by partnering with a reliable document destruction provider and direct employees to bring all paper documents and digital media to the workplace for proper disposal and destruction.

2. Beware of Unsecure Connections: Never use public Wi-Fi for sensitive work information. Using shared or public connections in business lounges or coffee shops can lead to data breaches. Establish policies that encourage employees to connect only to trusted networks for work purposes.

3. Travel with Care: Business travel is a fact of life these days, and in many ways, has become routine. According to cybersecurity experts, it's become easier for fraudsters and hackers to read the barcodes on boarding passes and gain access to passengers' contact information, future travel plans and frequent flyer accounts. Organizations should consider instituting policies that require employees to shred boarding passes, itineraries and other flight-related documents. Organizations can also encourage employees to use RFID blocking sleeves to protect credit cards and identification while travelling.

4. Keep it Private: Visual hacking of information on mobile devices can occur almost anywhere. Provide employees with privacy screens for laptops, tablets and other mobile devices to keep confidential information safe from prying eyes.

5. Protect Devices: Ensure all laptops and mobile devices are encrypted and password protected. Securing a laptop or other device means never leaving it unattended in a public place, car, or hotel room. When removing information from the workplace, encrypt files.

6. Beware of Complacency: Keeping information secure is a serious challenge and one that is constantly evolving. The risks are real and ever-present. Accordingly, organizations should fight complacency and ensure that they are creating a culture of responsibility within their organizations.

[5] https://www.idc.com/getdoc.jsp?containerId=prUS25705415

Ask the Expert

Andrew Lenardon, Global Director at Shred-it International shares his insight on the value of a comprehensive information security policy and what organizations around the world should be doing to help protect their workplace.

Why should businesses be concerned about their information security habits?

AL: Without proper protocols in place for protecting information, whether documents or hardware, companies run the risk of exposing themselves and their customers every day to serious data breaches. Globally, the average cost of a data breach is $4 million to recoup damages and the average cost for each record lost is $158[6]. When you factor this in, along with the business disruptions a breach may cause, one security incident can have a significant impact on the financial health of an organization.

However financial damage is not the only issue business leaders should be concerned about. Intangible aspects such as customer trust, organizational reputation and sustainability can be greatly affected by a data breach. Trust and reputation are considered to be among the most valuable of corporate assets, and if broken can cause detrimental damage to a business's ability to build a positive relationship with stakeholders.

How can a data breach affect organizational reputation?

AL: Quite simply, it all comes down to trust. Organizations around the world interact with customer data on a daily basis and customers rightly expect that their personal information is being protected. An information breach is also a breach of trust which can seriously damage an organization's reputation. Employee training and protocols help to mitigate this risk, but there is no magic bullet. Organizations need to be ever vigilant to protect their reputations and maintain customer trust.

[6] 2016 Ponemon Cost of a Data Breach, Page 1

Ask the Expert

What are the biggest barriers to addressing information security within an organization?

AL: It's two things. Firstly, if management does not demonstrate a commitment to security, employees won't take information security policies seriously. Business leaders must do their part to create a culture of security so that all employees understand the protocols in place for protecting confidential information. And secondly, personal accountability. Each and every one of your employees has to understand how their actions can put the company and its customers at risk. Something as simple as improperly discarding a document in the recycling bin when it may contain customer information creates liabilities and risk for a company. When all employees understand how to manage and identify privacy risks, business leaders are in a better position to protect their customers, their reputation and their people.

How can organizations meet the challenge of better protecting their information?

AL: Businesses of all sizes need to be proactive in addressing risk. In terms of information security, that means introducing protocols for proper document and hardware management that address everything from collection to storage and eventually destruction.

Business leaders prioritize regular employee training and policy auditing in order to protect workplace information security. Regular training and auditing not only mitigates the risk of data breaches caused by human error or lack of knowledge of security practices, but also serves as a helpful reminder to employees to follow policies. When all employees understand how to manage and identify privacy risks, business leaders are in a better position to protect their customers, their reputation and their people.

To keep employee, customer and company data safe these policies need to address confidential data inside and outside of the office. Information is still susceptible even if it's electronic; with the prevalence of electronic devices, like smart phones, tablets and laptops, it's becoming increasingly difficult to prevent confidential material from leaving the office.

Why should businesses be concerned about a growing mobile workforce?

AL: The more mobile – and global – workers become, the greater the amount of risk. As a result, C-Suite and SBOs must manage through these new challenges.

In a mobile workforce, business information is being stored on laptop hard drives, USBs, external hard drives or cloud networks and employees are taking their work away from the office. While the introduction of these devices allow employees to work off-site, it also means an immense amount of confidential information is leaving the office with them. Each of those technologies can easily be lost, left in a vehicle or accessed by hackers. A single lost or stolen laptop has the potential to seriously damage any business.

Additionally, employees are now accessing business documents and emails on computers and mobile devices that are not owned by the company. This may result in employers having less direct control over company information which can give rise to privacy, confidentiality and security risks. An employee working on his or her personal computer at home may not be as diligent about applying security updates and patches as the employer would be for its own institutional machines. This could leave workplace systems vulnerable to malware or spyware.

Companies should also caution employees to only take or print confidential information outside the workplace when absolutely necessary and instruct them on proper secure disposal. Digital information is not the only asset leaving the office with a mobile workforce and employees must understand and take appropriate precautions when removing any data from their workplace.

Privacy Protection – Think Global, Act Local

The old adage that a strong offence is often the best defense also holds true when it comes to privacy protection. Around the world, lawmakers are regularly updating rules or creating new policies to protect citizens and help ensure their personal information remains private.

Privacy Protection – Think Global, Act Local

The scale of the challenge is significant. Almost every government department or private business has information that should be securely stored and destroyed once no longer needed, for both privacy protection and regulation purposes.

According to global law firm DLA Piper, we are in a period of unprecedented activity in the development of data protection regulation around the world which will have a profound impact on the way in which global businesses are required to approach the collection and management of personal information[7]. Furthermore, the firm's Data Protection Laws of the World study suggests that the emergence of laws in countries which previously had no data protection law in place could create considerable enforcement risk in the future.

Businesses and organizations around the world need to be aware of the privacy protection regulations that govern their local operations. While health and financial-related data tend to be the most cited categories for regulations, many businesses rely on the expertise of a third party expert to review critical functions and identify the key areas of risk.

The chart below highlights typical functions within a business that could fall under privacy protection enforcement risk:

DEPARTMENT	WHAT NEEDS TO BE PROTECTED	RISKS
Human Resources	• Job applications • Health and safety documents • Medical records • Payroll information • Performance appraisals • Training information and manuals	Many HR documents contain the confidential and personal information of current and potential employees.
Sales/Marketing	• Customer lists and contracts • Financial information • Application forms • Strategic plans • Product samples • Launch calendars • Budgets and forecasts	Sales and Marketing materials often contain the private and confidential information of prospective and current clients. Additionally, they may contain business strategy and other intellectual property that should remain confidential.
Accounting	• Contracts • Invoices • Customer lists • Internal reports • Payroll statements • Supplier information • Financial applications	These materials typically contain financial information which if compromised, can cause significant damages.
Information Technology	• Hard drives • Memory Sticks • CDs • Zip disks • Network configuration details	Digital assets can contain millions of individual records and can inflict significant damage on an organization if lost or stolen. Electronic records can also be transferred or disseminated much more easily than paper- based materials.

[7] https://www.dlapiperdataprotection.com/#handbook/world-map-section

Privacy Protection – Think Global, Act Local

DEPARTMENT	WHAT NEEDS TO BE PROTECTED	RISKS
Procurement	• Corporate records • Supplier purchase orders • Supplier records • Supplier specification documents • Credit card information • Financial applications	Similar to accounting, the procurement department works closely with financial and historical records for the business as well as for its suppliers.
Research & Development	• Appraisals • Product test results • Formulas • Product plans • New product information • Reports • Specification drawings • Prototypes	This department manages intensely competitive information that can seriously impact an organization's competitive edge.
Management	• Budgets • Correspondence • Customer lists • Legal contracts • Forecasts • Strategic plans	Management typically works with highly confidential and sensitive materials.

Best Practices

Once organizations clearly understand their local legal obligations and have performed a comprehensive assessment of their risks, they can consider incorporating several best practices including:

- Establishing detailed policies and procedures to govern how the organization collects, manages, retains and destroys confidential information.
- Developing comprehensive training for staff on risks and processes to help them understand their role in securing private information.
- Securing all electronics – when they are in use and once they've outlived their lifecycle.
- Conducting regular audits to monitor effectiveness and compliance while regularly updating procedures and protocols

Summary

Shred-it is proud to provide actionable intelligence on the global technology, business, and policy trends that impact information security. As detailed in the Global edition of the 2016 State of the Industry Report, mobile technology has fundamentally changed the workplace. Now, businesses of all sizes must contend with many new challenges related to increased flexibility for employees and the growth of a mobile and increasingly global workforce.

The report highlights a number of these emerging challenges and offers solutions based on industry leading best practices. Some of the key takeaways for business leaders include ongoing training to familiarize employees with policies and procedures related to information security, developing policies and procedures to help manage the tools of the modern remote workforce as well as incorporating proper hardware management practices in an organization's overall approach to information security.

When it comes to protecting information security, complacency is among every organization's key risks. To ensure that their information security policies keep-pace, C-Suites and SBOs alike need to continue to take a broad view of information risks and impacts, as well as revisit their strategies regularly.

See how Shred-it can help improve your organization's information security by visiting shredit.com and selecting your region.

You can also stay informed with Shred-it online:

facebook.com/shredit

in linkedin.com/company/shred-it

@Shredit