SECURING THE FUTURE

In this Issue

The Current State of Data Security

Data security continues to dominate the headlines in the UK with news that companies, big and small, across an array of industries, are falling victim to security breaches. These breaches can range from accidentally misplacing customer information to occupational data theft and fraud. With a focus on protecting the confidential information of employees, customers and their organisation, business leaders need to recognise that information security policies and procedures are crucial to protecting their business.

Organisations or individuals that have access to personal data and operate in the UK are required by law to follow the Data Protection Act (DPA). As new threats to data security emerge, governments are required to revise and develop new regulations to protect the personal information of organisations; however, in an ever-changing landscape, businesses struggle to keep up with changes to legislation, placing them at risk of failing to meet information security requirements.

Since April 2010, the Information Commissioner's Office (ICO) has issued over £7.5 million worth of fines to organisations that have committed data breaches.[1] Our 2015 Shred-it Security Tracker survey found that while more companies are aware of the importance of data security, awareness does not always translate into action.

The Security Tracker also found that 98 per cent of C-suite executives and 88 per cent of small business owners are aware of the legal requirements concerning confidential data; however, a shocking 27 per cent of small business owners reported having no protocol in place for the secure destruction of confidential information. The gap between large organisations and small businesses is even wider for off-site working policies, with 53 per cent of larger organisations reporting having both an off-site and working from home policy in place, compared to only 33 per cent of small businesses.

Without the proper information security protocols and policies in place, organisations are not only risking the personal and confidential information of their customers and employees, but also increasing their chances of financial loss, reputational damage and legal repercussions.

No matter the size of the business, all organisations should develop and implement comprehensive policies that are aligned with legislative requirements and aimed at protecting sensitive data in all forms and at all stages of its lifecycle – from collection through to storage and destruction.

To get the facts about current security views, risk factors and prevention strategies in this year's State of the Industry report please visit the Shred-it Resource Centre to download the full report.

Training Employees on Information Security

Information security policies and procedures are vital when it comes to protecting small businesses from the risk of a data breach, but many small businesses are not doing enough to safeguard themselves against breaches from within their organisation and as a result human error remains a big risk within the workplace.

According to the 2015 Shred-it Security Tracker, 24 per cent of small business owners claim that human error, such as leaving sensitive information on desks, poses the biggest security threat to their organisation. Worryingly, 27 per cent of small businesses do not have information security policies and procedures in place and a third of those who do admit to never training their employees on these protocols. This highlights that many small businesses overlook the importance of data security training for their employees, particularly when it comes to spotting potential human errors before a data breach occurs.

Lack of workplace training can damage a company's reputation and threaten the security of a business. Our Security Tracker found that 32 per cent of small business owners say that they possess no information that would cause their business harm if stolen; however every business in the UK holds some form of confidential data – from payslips, meeting agendas to employee or client records. This suggests that there is a lack of awareness among small businesses about the different types of confidential data that, if not securely destroyed or stored, could lead to a damaged reputation, financial loss and legal fines.

It's important for small businesses to realise that they must take steps to help their employees understand information security responsibilities through information security protocols and training. From teaching employees to dispose of all documents securely, to mandating the encryption of mobile devices, arming employees with the knowledge they need helps protect organisations from the risk of fraud.

Shred-it helps small business owners protect their organisations with easy to execute tips for how to prevent a data breach. To find out more about how to become more secure, you can find helpful information on the Shred-it Resource Centre and we suggest following these tips:

- Schedule regular information security audits to identify problem areas and solutions.
- Introduce a Shred-it All Policy, which means all documents are destroyed prior to disposal or recycling.
- Keep an inventory of all information that needs to be protected.
- Schedule on going training so employees understand best practices for protecting confidential information – in and out of the workplace.
- Ensure employees are informed about the risks associated with data protection breaches and are well trained on which documents they should shred and how to securely dispose of electronic data.

Data Breach Roundup

In each edition we feature high profile data breaches to show businesses how they can mitigate similar risks.

This quarter we are highlighting Anglesey County Council.

Anglesey County Council was recently ordered to improve its data protection practices after it repeatedly failed to address security and privacy issues. Two separate security incidents as far back as 2011 led to the council signing undertakings to make changes and improve practices. But despite committing to the improvements, audit visits in July 2013 and October 2014 still found problems with the security of personal data. The ICO reported that the Council violated the Data Protection Act as it failed to take appropriate security measures against the unauthorised or unlawful processing of personal data. It failed to protect against the loss, destruction and damage to confidential information.

The Council maintains that it has now put measures in place to comply with data security provisions, such as: implementing a mandatory data protection training programme for all staff, ensuring staff understand and comply with protocols, backing up sensitive data, and implementing a clear desk policy.

What you can do: Privacy breach management is an essential part of a comprehensive privacy breach management programme. While many businesses are practicing strong information security procedures, there is still room for improvement around the secure storage and destruction of confidential information. There are simple steps a company can take to reduce the risk of a data breach and protect the information of their company and their customers.

1) Provide locked consoles for employees to dispose of information.
2) Provide clear protocols for the disposal of information that is no longer needed and of unused electronic storage devices.
3) Ensure employees remove portable devices from the office only when necessary and that those portable devices are encrypted.
4) Don’t allow people to keep unsecured documents on their desk and be sure to implement a Shred-it All Policy for unused documents.
5) Implement mandatory training and routine refreshers on information security policies and procedures.
6) Regularly revisit security policies and procedures to ensure they remain compliant with the latest privacy legislation.

Customer Connections

Shred-it's most important relationship is with its customers, which is why Shred-it Partners are trained to provide top level customer service and expertise. In each edition we highlight a Shred-it Partner that went above and beyond to provide exceptional customer service.

Wayne Keenan, CISP

Customer Service Representative (CSR), Newcastle

Earlier this year, Shred-it ran a contest to reward CSRs who went the extra mile in increasing awareness and improving customer experience.

Wayne was recognised for his efforts in helping his customers to find the Shred-it service that was right for them. For example, he helped audit a company's data security practices and advised on the best way for customers to store and destroy sensitive information.

> *"Huge congratulations goes to Newcastle CSR, Wayne Keenan who came out No 1 in the UK in the contest. Well done for being a Helpful Expert."*
>
> — Jason Potts,
> Customer Service Supervisor, Newcastle

Wayne said: "My role as a Shred-it CSR means that I'm responsible for providing our customers with an exceptional customer experience and that's something I take very seriously. It's important for me to listen to the needs of every customer and provide guidance to help them solve their problems. I once helped a customer with a console that was overfilling. I advised that having more than one would ensure that all confidential information was locked away safely, as well highlighting the cost effectiveness and how much time they would save from having to no longer move confidential data from one console to another. A crucial part of what I do as a CSR is developing a good, long-lasting relationship with my customers. Despite being a Shred-it partner for nearly a decade, I still experience a buzz whenever I help a customer."

For more tips on improving information security, please visit the Shred-it Resource Centre at shredit.co.uk/resource-centre

You can also stay informed with Shred-it on Facebook and LinkedIn or follow us on Twitter at @Shredit_UK

[1] Shred-it, *2015 State of the Industry Information Security United Kingdom*