SECURING THE FUTURE

In this Issue

Small Actions for Big Wins – The Information Security Checklist

It's no secret that in today's economic environment businesses have to be selective with their operational investments. Often it seems that if a programme isn't able to show an immediate increase in revenue, it's the first to be cut. But there's one area where it's always important to invest and that's information security.

With the cost of a data breach estimated at over £2.2 million per incident[1], organisations simply can't afford to overlook the importance of robust information security protocols and procedures. In Shred-it's fourth annual Security Tracker survey, nearly a quarter of both SMEs and large companies said they had never conducted an audit of the protocols they have in place.

Overlooking information security won't save money in the long run. Often, the costs incurred from regulatory fines, litigation, fraud and most importantly, the reputational damage that can result from a data breach, far exceed the cost of implementing a simple information security protocol.

1 Ponemon Institute, "2014 Cost of Data Breach Study: United Kingdom," May 2014

SECURING THE FUTURE

For these reasons, check out the Small Actions for Big Wins Information Security Checklist. The checklist outlines the most commonly overlooked information security practices to help businesses easily and affordably protect themselves from information theft and fraud.

You can download the Small Actions for Big Wins Information Security Checklist here.

Fight Fraud by Focusing on Your Office's Most Vulnerable Areas

Many business leaders don't know that one of the biggest sources of fraud comes from within the business itself. As a result, they often overlook key areas of vulnerability.

This year, to mark International Fraud Week, we've identified the top five most vulnerable areas within an office. The goal being to set business leaders up for success, so they can easily protect themselves and their customers.

The top five most vulnerable areas include:

1) **Printers:** Many offices do not require employees to use a security code to complete a print job, which means that confidential information is frequently printed and left at printing stations. In order to mitigate this danger, businesses should mandate that employees secure their print jobs by using a security code or allow employees printing confidential information to use a printer in their own office workspace.

2) **Non-Secure Recycling Bins and Wastepaper Baskets:** Disposing of data in an unsecure bin is just as risky as leaving it at a printer or on a desk. A shred-all policy eliminates the guesswork from the process and ensures that employees don't accidentally leave confidential information in unsecure locations. Of note is that shredded material is still recycled when using a third party provider.

3) **Messy Desks:** Messy desks with loose paperwork are vulnerable to snooping and data theft. They also expose confidential information to external staff, such as cleaners, who have access to the office or workplace. Consider implementing a clean desk policy and provide lockable storage units so employees can protect confidential information.

4) **IT Device Storage:** Electronic storage devices are very convenient when you can't access the company network, but they also raise the risk of fraud. Businesses can reduce the risk of fraud by requiring that storage devices be signed out and ensuring that they are securely destroyed when they reach the end of their use.

5) **Car/Homes/Hotels:** In the past, employees generally worked at the office and rested at home. With an increasingly mobile workplace, people can now access all their files at home. While convenient, that means that confidential information may be left in areas that are unsecure. Companies should caution employees to only take or print confidential information outside the workplace when absolutely necessary and instruct them on proper secure disposal.

As Workforces Go Mobile, Data Breach Risks Increase

As businesses move to improve employee satisfaction, productivity and work-life balance, there has been a significant shift towards remote working arrangements. In fact, the UK has seen a significant increase towards remote working arrangements within the last decade. In the last five years to 2013, there was a 13-percent increase in people working from home, according to a survey by the TUC[2].

While many employers recognise the positive effects of a flexible work programme, business leaders should be aware that this trend could have adverse effects on information security. Organisations need to be wary of allowing confidential information to leave the workplace and ensure all staff are mindful of data security risks when working from home.

Implementing preventative measures specifically for remote workers will help to safeguard an organisation's physical and digital assets. A well-understood information security policy, which includes remote working requirements, helps companies to address the extra risks associated with mobile working by ensuring that their information security protocol extends beyond company walls.

From encouraging staff to return confidential documents to the office for safe and secure disposal, to outlining best practice with respect to handling corporate devices such as laptops and mobiles, businesses need to provide clear rules to help employees maximise their productivity while also protecting sensitive information.

2 Trades Union Congress, "Home-working on the increase despite the recession", May 2013, www.tuc.org.uk

SECURING THE FUTURE

For tips on the mobile workforce, please visit the Shred-it Resource Centre for more information. You can also stay informed with Shred-it on Facebook and LinkedIn or follow us on Twitter @Shredit_UK.

Data Breach Roundup

Our pick of recent high profile data breaches and their impacts:

Ministry of Justice – This government ministry was fined £180,000 over serious failings in the way prisons in England and Wales have been handling people's information. The penalty follows the loss of a hard drive at a prison in Wiltshire. The drive was not encrypted and contained confidential information about 2,935 prisoners, including details of links to organised crime, health information, history of drug misuse and material about victims and visitors.[3]

Worldview Limited – The hotel booking website was fined £7,500 over a security breach involving its website that allowed hackers to swipe the full payment card details of some 3,814 customers. The unidentified attacker exploited a SQL injection flaw in Worldview's website to access the firm's customer database.[4]

Swale Council – Swale Council has suffered a data protection breach where the emails of roughly 2,500 residents were released in the public domain, breaking the Data Protection Act. The council is expected to be fined in line with similar breaches that have taken place including the breach at the Isles of Scilly Council.[5] Kent Online reports that the accident caused the information to be shared on a message advertising an e-billing system. The emails were delivered in batches of ten, with each comprising of around 250 contact details.

About Shred-it

Shred-it is a world-leading information security company providing information destruction services that ensure the security and integrity of our clients' private information. The company operates in 170 markets throughout 18 countries worldwide, servicing more than 300,000 global, national and local businesses. For more information, please visit shredit.co.uk

3 ICO, "Repeated security failings lead to £180,000 fine for Ministry of Justice", August 2014, www.ico.uk
4 John Leyden, "Watchdog bites hotel booking site: Over 3k card details slurped", November 2014, www.theregister.co.uk
5 Kroll Ontrack, "Swale Council data breach could lead to legal action", October 2014, www.krollontrack.co.uk