SECURING THE FUTURE

In this Issue

UK Businesses Not Turning Data Security Awareness Into Action

Information security awareness among businesses in the UK has improved since 2011, according to Shred-it's 5th Security Tracker survey. Over the last five years, there has been a steady improvement in knowledge with more organisations claiming to be aware of their legal requirements. However, the results also showed that this awareness is not translating into action, particularly among SMEs.

Awareness of legal data protection requirements is particularly high among larger businesses, with 98 per cent of C-Suite executives claiming to be in tune with these. While the level of awareness is high among SMEs, with some 88 per cent of SME business owners saying they are just as aware of these legal requirements, this awareness is not translating into action for the majority of small businesses.

Almost a third (27 per cent) of SME business owners claim to have no protocols in place for storing and disposing of confidential data compared to just 3 per cent of C-Suite executives. It is these larger businesses that are leading the way when it comes to taking action towards protecting the confidential data of their customers and employees from data breaches. Our Security Tracker results showed that over a third (35 per cent) of C-Suites have a locked console to store confidential data alongside a professional information destruction firm, compared to only 11 per cent of SMEs.

SECURING THE FUTURE

What is even more concerning is that despite claiming to be aware of the legal requirements for storing and destroying confidential data, the majority of SMEs are not so aware when it comes to identifying the potential impact of a data breach. Shockingly, only 10 per cent of SME business owners say that a breach would seriously impact their organisation. Considering the financial, legal and reputational repercussions that lost or stolen data could have on their business, it is alarming that 36 per cent of SMEs are not aware of the risks. Continue reading for some tips on how to protect your business.

Furthermore, Security Tracker findings reveal that this year, C-Suite executives are much more likely to say that their staff are trained on their organisation's information security procedures at least once a year. While SMEs are slightly ahead of where things began in 2011, the frequency at which they train their staff is down from 2014. This shows that more needs to be done to make sure that small businesses are given the right tools so they can be just as protected against data breaches as their C-Suite counterparts.

For more results from the Shred-it 2015 Security Tracker visit our Resource Centre.

Protecting electronically-stored data

As organisations refresh computer hardware and digital storage, they are faced with the issue of what to do with their obsolete IT assets. Proper disposal and destruction of hard drive storage devices is important not only to keep confidential information safe, but also to keep organisations compliant with laws and legislations regarding the storage and disposal of information.

While shredding paper information is an incredibly important part of preventing a data breach, information stored on electronic devices — such as hard drives, laptops or mobiles — must also be taken into consideration when securely disposing of confidential information. The most effective way to verify that confidential data found on these devices is completely irretrievable and not susceptible to a privacy breach is to securely destroy the hard drive before disposing of it.

However, the 2015 Shred-it Security Tracker revealed that 40 per cent of UK small businesses and 6 per cent of larger businesses have never disposed of hard drives, USBs or other hardware that contains confidential information. That translates into a lot of organisations that are not only risking the personal and confidential information of their customers and employees, but also risking compliance with regulations such as the Data Protection Act, which safeguards personal information.

It is critical that organisations protect confidential information, by removing and destroying unused hard drives. For simple workplace guidelines designed to safeguard hard drives, visit the Shred-it Resource Centre.

SECURING THE FUTURE

Data breach roundup

The first step towards fixing a problem is knowing that it exists. In each edition we feature a high profile data breach to show businesses how they can mitigate similar risks.

This quarter we are featuring Barclays bank.

Internal breaches continue to be a significant threat to businesses across the UK with 90 per cent of larger organisations suffering a data breach in the past twelve months (up from 81 per cent in 2014).[1] Unfortunately, businesses all too often overlook areas of vulnerability, particularly when it comes to information stored on electronic devices.

Recently, it emerged that a Sussex branch of Barclays bank left personal details of 13,000 customers in the hands of fraudsters for up to seven years. Police found a USB stick containing confidential customer information including: names, dates of birth, national insurance numbers, passport details and salaries. The bank is investigating whether the data was stolen by an employee.

The information, which dates from 2008, came from a defunct Barclays unit that sold investments and pensions. The bank is reportedly paying compensation of £4 million to the victims of the data theft. This is not the first data breach from Barclays to occur from a misplaced electronic device. In 2014, another memory stick was discovered containing files with information on 2,000 Barclays customers.

This year, our Security Tracker revealed that 72 per cent of C-Suite executives and 23 per cent of small business owners are concerned about the possibility of employees stealing confidential customer or company information. However, there are concrete actions business leaders can take to lower the risk of fraud and become more secure including:

- **Implement a clean desk policy:** Without a clean desk policy or lockable consoles for employees to protect confidential information, paperwork or electronic devices are vulnerable to data theft, and could be left available to outside staff such as cleaners or even members of the public.
- **Revisit and assess existing policies:** The best way to improve security in an organisation is to conduct frequent audits to ensure that policies and procedures being followed and are able to combat threats as they emerge.
- **Don't allow non-secure recycling bins and wastepaper baskets:** Disposing of information in an unsecure bin is just as risky as leaving it at a printer or on a desk. A shred-all policy ensures that employees don't accidentally leave confidential information in unsecure bins. A third-party provider will also ensure that the material is recycled and safely destroyed.
- **Secure 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 unattended on or around printers or photocopiers.
- **Securing electronic devices:** Employees need to ensure that any electronic device used outside the confinements of the workplace, such as a USB stick, is monitored at all times to prevent theft.

SECURING THE FUTURE

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. An important part of this is fostering opportunities within the company and helping our Shred-it Partners to work as a team in order to deliver great customer service.

In this edition, we highlight a Shred-it Partner that has shown great commitment to the Shred-it team and to our customers.

Paul Playle, CISP

Sales Manager, Newcastle

Paul joined Shred-it eight years ago as a Sales Executive and as a result of his hard work he has recently been promoted to a managerial role.

Shred-it would like to congratulate Paul for his hard work in attracting new customers and motivating the members of his team.

"Within Shred-it, there is constant innovation across the business, which helps encourage me — and others on my team — to grow and provide great customer service. Since progressing into a managerial role, I have mentored over 30 people across the business, helping them to find new ways to solve our customers' challenges so that businesses across the UK can improve their information security. There is a good level of trust between team members here and we work together to provide every customer with expert knowledge on how to reduce the risk of a data security breach"

— Paul Playle,
Shred-it Sales Manager

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. PWC, *The Global State of Information Security Survey 2015*