SECURING THE FUTURE

In this Issue

Businesses Should Avoid Making These Common Mistakes

The first step in improving information security is conducting a thorough assessment of the vulnerabilities in your business. However, according to the 2014 Shred-it Information Security Tracker, **over 75 per cent of UK SMEs** are at risk of disposing of confidential information in the wrong place.[1]

Take a close look at your organisation's current information security procedures so you can identify any potential mistakes and take concrete action to lower your risk.

Here are the top ten mistakes businesses make:

1. **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 eliminates the guesswork of what is and isn't confidential from the process and ensures that employees don't accidentally leave confidential information in unsecure bins.

2. **Allow employees to leave documents on their desks or in unlocked filing cabinets:** Without a clear desk policy or lockable storage units for employees to protect confidential information, any paperwork is vulnerable to snooping and data theft, and available to outside staff such as cleaners and building contractors.

SECURING THE FUTURE

3. **Don't 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 at printing stations. Also, businesses often overlook physically destroying hard drives on printers at the end of their use, not realising that the information that's been printed is stored in the printer's memory.

4. **Allow employees to remove confidential information from the office:** With an increasingly mobile workplace, people take their work home with them. 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.

5. **Allow employees to use personal smartphones without reviewing security measures:** Smartphones allow employees to work from almost anywhere. They also allow another point of access to potentially confidential material. If your company doesn't require the use of passwords (at a minimum) or encryption as part of your cyber security plan – even if the device being used belongs to the employee and not the company – the risk of a data breach increases significantly.

6. **Don't properly manage IT devices:** 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, such as memory sticks and portable hard drives, be signed out and ensuring that they are securely destroyed when they reach the end of their use.

7. **Use whiteboards and flip charts for team projects without clearing them:** A collaborative workplace can result in increased productivity and innovative thinking. However confidential information left on whiteboards or flip charts can increase an organisation's security risks as the information is available in common areas for any passerby to see. It's important to ensure policies extend to the clearing of whiteboards and secure destruction of flip chart pages to ensure information doesn't fall into the wrong hands.

8. **Allow password sharing on shared accounts without clear transition policies:** Using a shared online account between multiple employees is convenient and can limit the number of accounts in use. However, using a common password that multiple people know increases vulnerability, especially when an employee leaves the company.

9. **Don't train your employees:** The best information security policy is the one that employees follow. If employees don't understand how or why to follow a policy, it's pretty much dead on arrival. By investing the time in helping employees follow the rules, your company is investing in real security.

10. **Don't regularly revisit and assess existing policies:** As organisations change and grow, so do their information security risks. While many business leaders will include risk assessments of new programs at the onset of implementation, it is important to regularly revisit security policies and procedures to ensure they reflect the realities of a constantly changing business.

SECURING THE FUTURE

Fighting the Fraudsters

Every year businesses across the UK lose millions of pounds to online, mail, door-to-door and telephone scams. This type of fraud can cause devastating damage to businesses. It's important to stay informed so you can recognise these scams and protect confidential information.

Small businesses are often targeted by unauthorised directory listings or advertising fraud in an attempt to bill the organisation for an advertisement or directory listing which does not exist. The organisation is deceived by a fake quote based on a genuine entry or advertisement the business has had in a different publication or directory.

You can protect your business by implementing simple measures including:

- Ensuring that employees processing invoices or answering calls are aware of these scams.
- Always checking that goods or services were both ordered and delivered before paying an invoice.
- Never giving out or updating any information about your business unless you know what the information will be used for.
- Not agreeing to a business proposal over the phone – always ask for an offer in writing.
- Limiting the number of employees who have access to funds and have the authority to approve purchases.

For more information on how to recognise fraud you can visit the ActionFraud website and take a look at these tips on how to protect your business against fraud.

Data Breach Roundup

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

This quarter we're highlighting:

"Strike week" is a March 2015 initiative by the UK's National Crime Agency. This initiative saw 56 suspected hackers arrested as part of the ongoing fight against cybercrime. More than 25 operations were carried out across England, Scotland and Wales, with arrests including a man suspected of involvement in a 2012 hacking attack on Yahoo.

What you can do:
Cybercrime continues to be one of the biggest threats to businesses, however according to the 2014 Annual Shred-it Security Tracker, 50 per cent of UK firms surveyed reported having no cyber security policy in place. It is important for business leaders to ensure their information security protocols extend to include cyber security and the disposal of e-media and hard drives. Erasing hard drives does not mean data is destroyed. Physical hard drive destruction is proven to be the only 100 per cent secure way to destroy data from hard drives.

SECURING THE FUTURE

Customer & Community Connections

Shred-it truly values its relationships with its customers and the communities in which it operates. This is why Shred-it Partners are trained to provide top level customer service and make a positive contribution in their local communities. In each edition we highlight Shred-it Partners who went above and beyond to provide exceptional service to these groups:

Paul Marra
Edinburgh branch

Last year, Shred-it's Edinburgh branch set up a relationship with their local primary school. Pupils have now visited the branch three times to see the shredding process and discuss how Shred-it helps the environment by recycling all of the shredded paper. Over Christmas, Paul Marra of Shred-it visited the school to discuss how they could help over the holidays by filling our bags with their Christmas wrapping paper and cards. When they were full, the class stopped by to see their bags being shredded. Over 80 bags were given to Shred-it by the school. Paul also showed them videos about the shredding and recycling process and discussed Shred-it's environmental policy.

Shred-it would like to commend the Edinburgh team for this innovative initiative and the contribution they're making to local community life.

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 Ipsos Reid, 2014 Information Security Tracker