SECURING THE FUTURE

In this Issue

- UK businesses at risk from inadequate disposal of electronically-stored information
- Businesses lack knowledge — part of the problem!
- What should your company do in the wake of a data breach?
- Further information and advice

UK Businesses at Risk from Inadequate Disposal of Electronically-Stored Information

In this issue, we discuss how UK businesses are putting their information security at risk through long-term storage of electronic devices containing confidential information.

Sometimes it's easy to forget that confidential information stored on electronic devices needs to be disposed of as thoroughly and securely as sensitive information recorded in paper form. With cyber security a growing concern and the ubiquity of electronic devices used by today's mobile workforce, it's simply good business sense to take into account confidential information stored electronically when considering your overall information security plan.

In Shred-it's fourth annual information Security Tracker survey, we discovered that UK SMEs are putting the confidential information of their customers and employees at risk by not disposing correctly of redundant electronic devices containing confidential information. In fact, 32 per cent of SMEs say they have never disposed of these, while another 35 per cent say they do so less than once a year! On top of this, our study also shows that 51 per cent of SMEs do not have a cyber-security policy in place despite a number of high-profile security breaches this year in the UK.

SECURING THE FUTURE

Businesses lack knowledge — part of the problem!

Part of the problem could be that SMEs are lacking knowledge about what constitutes confidential information. Our survey found that 21 per cent believe they possess no documents that would cause their business harm if stolen, despite the vast array of commonly-held information that should be treated as confidential — from employee records to client invoices! When you think that only 46 per cent of SMEs could correctly identify the potential financial penalty for breaching the Data Protection Act – it's up to £500,000! — then there is definitely some cause for concern.

When it comes to larger companies, 35 per cent of business leaders admitted that they disposed of electronically-stored information either less than once a year or never. However these companies were more likely to have a cyber-security policy in place (77 per cent).

With all businesses facing significant damage to hard-earned reputation as well as financial penalties from the Information Commissioners Office (ICO) of up to £500,000, it is absolutely critical to include electronically-stored confidential data in your information security policy. Regardless of your business' sector, size or location, you need to recognise that you have a responsibility to safely dispose of confidential information held on electronic devices, such as laptops, mobile phones, hard drives and portable storage devices.

Three simple workplace guidelines designed to safeguard hard drives:

- Perform a regular clear out of storage facilities and avoid stockpiling unused hard drives;
- Destroy all unused hard drives using a third-party provider who has a secure chain of custody to help give you peace of mind and ensure your data is being kept out of the hands of fraudsters;
- Regularly review your organisation's information security policy to incorporate new and emerging forms of electronic media.

What types of electronic media can be destroyed?

- Hard Drive (any kind of laptop, desktop, PATA, SATA and many more).
- Backup Magnetic Tapes (any kind of DLT, mini cartridges and many more).
- Floppy Disk (3.5 inch disk, 5.25 inch disks, and many more).
- Zip Disk (100 MB, 250 MB, and other large disks).
- Optical Media (CDs, DVDs, Blue Ray, and HD DVD).

SECURING THE FUTURE

Are you doing enough?
To take control and properly manage your confidential data, keep the following suggestions in mind:

- Demonstrate a top-down commitment from management to the total security of your business and customer information.
- Implement formal information security policies; train your teams to know the policies and strictly follow them.
- Eliminate potential risk by introducing a "shred-all" policy; remove the decision-making process regarding what is and isn't confidential.
- Conduct a periodic information security audit.
- Introduce special locked consoles instead of traditional recycling bins for disposing of confidential documents.
- Don't overlook hard drives on computers or photocopiers. 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.

A 2014 survey of UK businesses carried out on behalf of the Department of Business Innovation & Skills (BIS) found that some 81 per cent of large corporations and 60 per cent of SMEs had a data breach in the last year. Therefore it's clear that organisations need to prioritise information security by implementing protocols that help protect documents and hardware.

What should your company do in the wake of a data breach?

If your organisation experiences a data breach, there are a few important steps that should be taken immediately:

- Seek expert legal assistance and advice.
- Take inventory of the data that has been impacted.
- Develop a targeted plan of action that includes clearly-defined steps.
- Carefully manage the flow of information related to the breach.
- Be prepared to communicate effectively to all stakeholders, including customers, partners, vendors, employees, the media and if needed, the Information Commissioners Office.

Quick corrective measures are essential, but it is also critical for companies to take proactive steps to prevent further breaches from occurring.

SECURING THE FUTURE

Further information and advice

To learn more about complying with data protection and information security legislation visit: shredit.co.uk/resource-centre.

You can also book a FREE Data Security Survey with a trained Shred-it representative to help you uncover potential risks in your current secure destruction processes.

Stay informed with Shred-it on Facebook and Linkedin or follow us on Twitter @Shredit_UK.

About Shred-it

Shred-it specialises in providing a tailored document destruction service that allows businesses to comply with legislation and ensure that their client, employee and confidential business information is kept secure at all times. Shred-it provides the most secure and efficient confidential information destruction service in the industry.