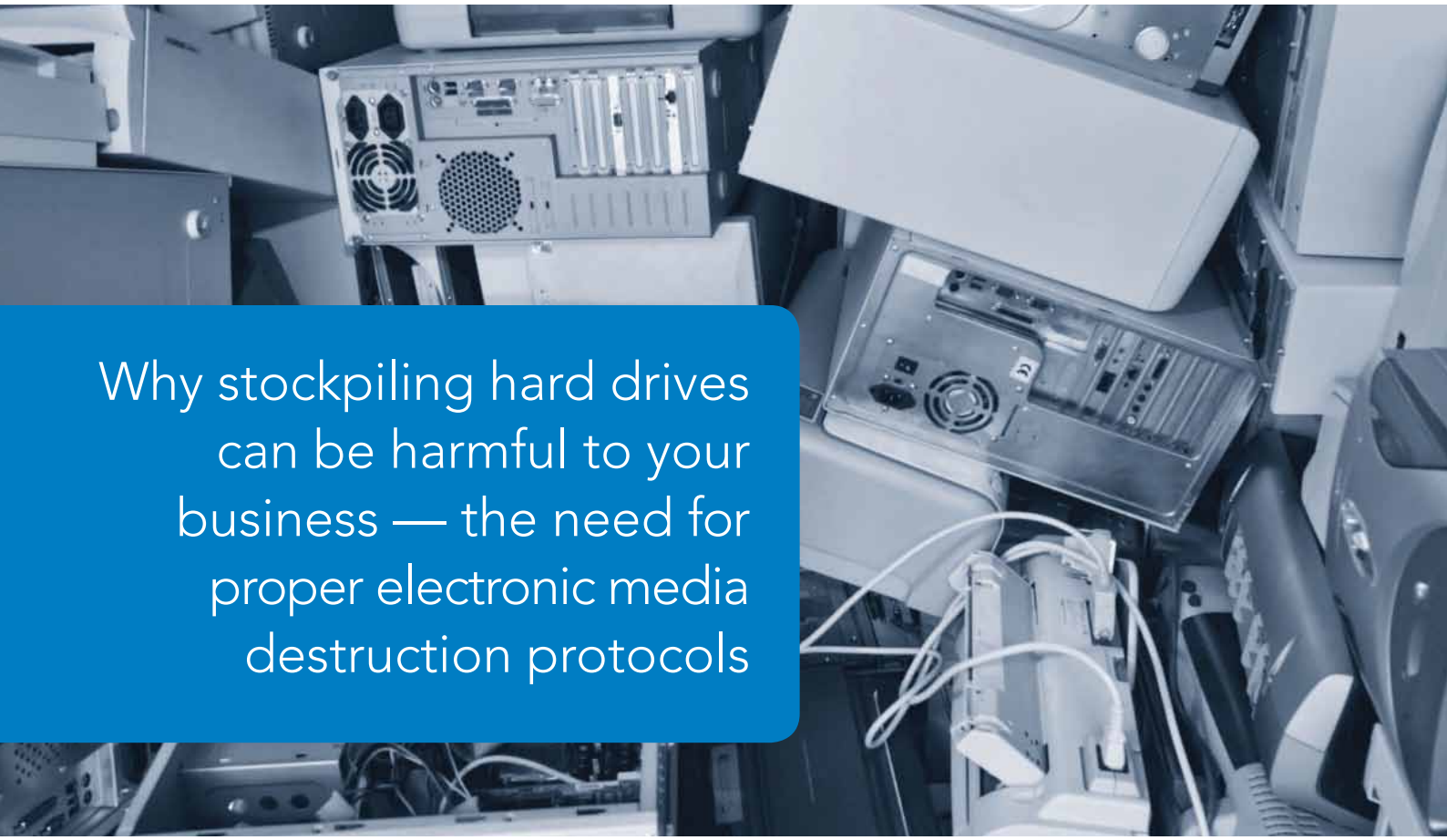
SECURING THE FUTURE

In this Issue

- It's under lock and key so it's secure, right?
- This would never happen to our company!
- Why put your company at risk?
- What types of electronic media can be destroyed?
- Shred-it's hard drive destruction services
- Your free security consultation



Why stockpiling hard drives can be harmful to your business — the need for proper electronic media destruction protocols

In this issue, we will discuss how stockpiling your old hard drives makes your organisation more vulnerable. This begs the question: why take the risk?

Many British businesses, both large and small, may not realise that the most effective way to properly dispose of hard drives and electronic media is to destroy them. The issue is new enough that many companies' security protocols and procedures don't account for unused hard drives and electronic media. Instead, businesses often stockpile items with confidential information on them indefinitely, locked away in a cupboard or storage area. Shred-it's 2015 Information Security Tracker survey, which assessed the opinions of small and large businesses, discovered that 6% of large organisations and more than a third of small ones (40%) have never disposed of hardware containing confidential data.[1] Despite both the short and long-term negative consequences, many UK businesses appear to follow this process because they are unaware of the risks to themselves and their customers.

SECURING THE FUTURE

It's under lock and key so it's secure, right?

As technology evolves, misconceptions have emerged about hard drive and electronic media security. For example, locking up old hard drives in an IT store room or an off-site storage facility is often perceived as a safe option, despite being a target for data thieves. Even if organisations use software to erase, wipe, reformat and degauss electronic devices, it may not fully protect you – confidential data from obsolete hard drives can still be retrieved and end up in the wrong hands. Carelessness is just as dangerous, with improper destruction potentially leading to a costly breach that could damage your company's reputation. This begs the question, why risk it?

Shred-it's Information Security Tracker found that 50% of UK businesses mistakenly thought that erasing, wiping or degaussing their devices before recycling them was enough to protect their confidential information from being lost or stolen. Another 14% of British businesses indicated that they simply recycled their old electronic media. Further, 13% said they didn't know how their business was disposing of its ageing or obsolete computers, or other data-storing devices such as smartphones or photocopiers. Given the importance of destroying a hard drive, it's startling to think that **only 23% of businesses across the UK reported using this method of destruction.**

But we are secure — this would never happen to our company!

Could it though? In June 2012, the Information Commissioner's Office (ICO) fined a hospital trust £325,000 after computer hard drives containing confidential information on thousands of patients were stolen. Sensitive personal data was discovered on hard drives sold on an internet auction site. The hard drives contained staff details including national insurance numbers, home addresses, ward and hospital IDs, and information referring to criminal convictions and suspected offences.[2]

Just over a year later, in July 2013, another hefty penalty of £200,000 was levied against another NHS trust following the discovery of thousands of children's patient records on a second-hand computer that was auctioned online. Regulators said NHS Surrey failed to check that a data destruction company had properly disposed of the records. The data destruction company had offered free disposal of the computers in exchange for the sale of salvageable materials and had promised to crush the hard disks, but the health trust had failed to monitor the destruction process, the ICO ruled, and did not have a contract in place that explained the legal requirements of the data destruction.[3]

You might be quick to point out that this is not your business as this occurred in the public sector and you may think that it wouldn't happen to you. However, in 2014 the UK's private sector accounted for more than a third of all reported data breaches and more than half of the resulting fines (57%).[4] You may follow policies and procedures, but do all of your employees do the same? The information breach has once again raised red flags around workplace policies and procedures.

Below is a list of best practices to implement in your workplace to avoid data theft:

- Consider performing regular clean-outs of storage facilities and avoid stockpiling old, unused hard drives. The Data Protection Act stipulates that personal data should not be kept for longer than the purpose for which it was collected in the first place — so even the simple act of storing them could mean you are breaking the law

SECURING THE FUTURE

- Destroy all unused hard drives at the end of their useful life. If using a third-party provider to do this for you, check they have 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
- Consider conducting regular reviews of your organisation's information security policies to incorporate new and emerging forms of electronic media and ensure your staff training also covers this high risk area

Why put your company at risk?

The cost to destroy hard drives is minimal when compared to the potential risks faced when you don't. Shred-it, the world leader in secure information destruction, can permanently destroy confidential information at a low cost that will fit your budget. Not only that, hard drive destruction is the most effective way to permanently destroy all information. Shred-it's secure chain of custody guarantees secure destruction, with a Certificate of Destruction issued for your files. At the end of the day, Shred-it's Hard Drive Destruction Service will offer more than just a certificate; it offers the peace of mind you deserve.

Shred-it's Hard Drive Destruction Service fully destroys hard drives, memory sticks and photocopier memories, rendering them completely useless and beyond repair. This offering also allows businesses and IT professionals to track their information destruction history through our unique barcode scanning technology.

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 disks, 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 DVDs)

0800 028 1164 | shredit.co.uk

Shred-it

Making sure it's secure.™

SECURING THE FUTURE

Why should you consider Shred-it's Hard Drive Destruction Services?

✓ 100% DESTROYED	Only destroying your hard drives ensures they are useless to identity thieves
✓ 100% SECURE	Shred-it's full chain of custody process provides end-to-end security
✓ 100% ASSURED	Shred-it will provide an itemised Certificate of Destruction for you to keep for your files
✓ 100% PEACE OF MIND	Shred-it offers a risk-free alternative to stockpiling, erasing, reformatting or degaussing obsolete or unused electronic media
✓ 100% SHRED-IT	Over 25 years of proven and total commitment to secure information destruction

Your FREE Security Consultation

Learn more about Shred-it's Hard Drive Destruction Services. Visit us at: shredit.co.uk/hard-drive

You can also visit Shred-it on Facebook and LinkedIn or follow us on Twitter @Shredit_UK.

1. Shred-it, 2015 Information Security Tracker 5.0
2. BBC News, 2012, Brighton Hospital Fined Record £325,000 Over Data Theft
3. BBC News, 2013, NHS Surrey Fined £200,000 After Losing Patients' Records
4. ICO, Action We've Taken, Enforcement

0800 028 1164 | shredit.co.uk

Making sure it's secure.™