In today’s business environment the majority of organisations are not paper free and it seems likely that it’ll be some time before this happens; Brits still use an average of 2.5 million tonnes of paper annually.\textsuperscript{1} Despite this, there are still some businesses that are moving towards a ‘paperless’ office, which means that they are relying heavily on devices such as hard drives to store information.

Unfortunately organisations often don’t realise that these devices are storing confidential and potentially damaging information and as a result may not be taking proper precautions in disposing of these devices. According to the 2014 Shred-it Security Tracker, 32 per cent of UK SMEs and 15 per cent of larger businesses surveyed have never disposed of hard drives, USBs or other hardware that contain confidential information, which translates into a large amount of confidential data that could potentially fall into the wrong hands.\textsuperscript{2}

Once a hard drive is unused, the only way to ensure that the data on it is completely gone is to remove the hard drive from its device and securely destroy the hard drive before throwing it away, recycling or selling it.

Three Simple Workplace Guidelines Designed to Safeguard Hard Drives:

1. Perform a regular cleaning of storage facilities and avoid stockpiling unused hard drives.
2. Destroy all unused hard drives using a third-party provider who has a secure chain of custody and confirms destruction, to help give you peace of mind and ensure your data is being kept out of the hands of fraudsters.

3. Regularly review your organisation’s information security policy to incorporate new and emerging forms of electronic media.

How Millennials Affect the Workplace and Data Security

Millennials are quickly becoming one of the most influential and dominant employee sectors in the workplace. Forecasters predict that 75 per cent of the UK workforce will be comprised of Millennials by the year 2025.3

With significantly different values than their predecessors, this generation does not seem to view data security as a serious risk to themselves or their workplace.

Despite being driven by technology, UK Millennials are less worried about companies having access to their data than their European counterparts.4 From an organisational standpoint, this lack of concern surrounding online security needs to be addressed and mitigated through company-wide policies related to smartphone apps and for personal devices used in a work capacity.

A further UK study into cybercrime reports that 34 per cent of millennials (aged 18 to 29) view data theft as a victimless crime compared with only 11 per cent of baby boomers (aged 55-plus).5 It seems that millennials aren’t aware that their company’s clients and employees can be the victims if there is a data security breach.

What’s more, more than 72 per cent of millennials believe they are entitled to take data they have worked on compared with 41 per cent of baby boomers.5 With an increase in flexible working, taking documents home may seem harmless to millennials but in some cases, documents can go missing and end up in the wrong hands.

It is clear that perceptions towards data security have changed, which is why workplace data security policies should aim to correct these misperceptions internally in order to prevent a data security breach.

For tips on how to keep confidential information safe, please visit the Shred-it Resource Centre shredit.co.uk/resource-centre for more information. You can also stay informed by reading the Shred-it blog or you can follow us on Twitter at @Shredit_UK.
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 wanted to feature an investigation currently underway at the Northumbria Healthcare NHS Foundation Trust.

Northumbria Healthcare NHS Foundation Trust: An investigation is currently underway following a data breach caused by a member of staff mistakenly faxing patients’ information to a member of the public. The Northumbria Healthcare NHS Foundation Trust has breached the Data Protection Act having wrongly sent five faxes containing information relating to the care of several patients.

In the past, the Trust has suffered a similar data breach and took action to make sure its fax machines were only able to send information to pre-programmed numbers belonging to organisations working in the health service. Unfortunately, the hospital failed to adopt this new data protection protocol across all wards leading to more confidential information being released to the public.

The Trust has since made a commitment to The Information Commissioner’s Office (ICO), which carried out the investigation, to ensure it improves the way it handles patients’ information in the future.

What you can do: The medical industry, among other organisations, need increased awareness around confidential medical records, and there are simple steps a company can take to reduce the risk of a data breach.

1. Provide clear protocols for the disposal of information that is no longer needed including unused electronic storage devices.
2. Ensure all employees are aware of your organisation’s data security protocols and are educated about data security risks.
3. Don’t allow people to keep unsecured documents on their desk, and be sure to implement a shred all policy for unused documents.
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. In each edition of our newsletter, we highlight our Shred-it Partners who have gone above and beyond to provide exceptional customer service.

Claire Hellen, Customer Care Executive & Martin Byrne, Customer Service Support — Portsmouth

Claire and Martin have done some fantastic work with a major aerospace firm in Portsmouth. They are both committed to consistently meeting and exceeding customer expectations, which has resulted in the company signing with Shred-it for three more years.

They have both gone above and beyond to ensure the needs of their customers are met, and in doing so, have helped make the aerospace firm a loyal customer.

Shred-it would like to commend Claire and Martin for their exceptional customer service work.

“Thank you to Claire Hellen and Martin Byrne for their fantastic work on a customer audit in Portsmouth, where Shred-it excelled in every aspect of the word.”

Sheridan Lott, Shred-it Senior 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. My Rutland, Facts and Figures
2. Ipsos Reid, 2014 Security Tracker, Why stockpiling hard drives can be harmful to your business
3. Microsoft, 2015, Mobile is Driving the Digital Revolution
4. Information Age, 2014, UK Millennials Less Wary of Sharing Data With Brands Than European Counterparts
5. Raconteur, 2015, Employee Engagement Can Be Defence Against Cyber Crime