What if you lost your laptop?

Did you know that there is a World Backup Day?

Well there is and it's 31st March each year! The day reminds us to protect our precious digital documents as we become more and more reliant on technology and stresses the importance of regular backups. The proposed solution is to backup all your data in three different places (3-2-1 strategy) – one copy on your computer/tablet, one on an external storage device (USB stick or hard drive) and another offsite on a cloud storage solution.

I am sure that like me you ALL back up your data regularly (yeah, right!) but when the time comes to replace outdated PC's or external hard drives how do you ensure that your precious data is not going to end up being accessed by criminals?

In a recent survey less than 20% of businesses across the UK said that they were shredding their computer hard drives. Over half the businesses thought that erasing, wiping or degaussing their hard drives before recycling them would completely obliterate the data and protect their confidential information from being stolen or misused. To complete the statistics 14% said that they simply recycled their electronic media without even wiping the data and 12% said that they had no idea how

their business disposed of it's out of date or obsolete computers, data storage devices or smartphones. When asked a staggering 72% of businesses did not know that most photocopiers have an electronic memory that can be used to reproduce exact images of all documents that have been copied on that machine using forensic software programmes (available free online).

It's a fact that the only way to completely destroy data held electronically is to destroy the hardware that carries the data.

Methods of destruction vary from incineration to turning hard drives into minute metal fragments (for more information see here)

"It would never happen in our company"

You may think that but British Airways was recently fined £20 MILLION by the Information Commissioner's Office after data was stolen which contained personal and financial details of more than 400,000 of it's customers Oct 2020 (read more about it here) . Although this particular data breach was a 'hack' of the main BA system, data being lost or stolen and unprotected by even basic password protection or encryption of laptops, external hard drives and USB sticks is depressingly common. Even as far back as 2013 household name businesses have received six figure fines for failing to take the appropriate measures to protect legacy customer data on their hard drives or USB's. Fines and reputational damage that follow the loss and exploitation of such data can ruin any business.

It is estimated that 91% of corporate laptops and desktops contain sensitive data and that the average **cost to rectify a single record breach is £219** in compensation and management/staff time. Massachusetts Institute of Technology (MIT) recently tested 158 used hard drives and recovered 92% of sensitive information which included credit card numbers, emails, medical records, names and contact numbers.

So what can you do?

It is worth implementing some best practices in your workplace to avoid data theft, including:

- Avoid stockpiling unused hard drives (laptop & desktop towers) USB's and disks particularly in unsecured locations
- Regularly clean out hardware storage facilities
- Destroy all unused hard drives/USB's/CD&DVD disks using reputable specialist providers who have a secure chain of custody which will provide you with peace of mind and will ensure that your data is kept out of the hands of fraudsters
- Regularly review your organisation's information security policy to incorporate new and emerging forms of electronic media

Scan Film or Store will permanently destroy all types of your electronic media utilising a secure chain of custody including collection by our own staff in our own vehicles, recording of the items serial numbers at point of collection and will issue a Certificate of Destruction for your files detailing what has been destroyed. Destruction methods vary according to the media type i.e. hard drives are turned into tiny metal chips whereas microfilm and magnetic computer tape is incinerated.(learn more about our services here)

We can destroy:

- Hard Drives (from any kind of desktops or laptops)
- USB/Pen
- Flash drives/Portable External Hard Drives
- Backup Magnetic Tapes (any kind of DLT, mini cartridges etc)
- Floppy Disks (both 3.5 and 5.25 inch disks)
- Optical Media (CD's, DVD's, Blu Ray and HD DVD's)

If you would like some free advice on how to protect your unused data please contact us here