Another Time Bomb Waiting To Explode

One cannot grasp the scale of the average company's data footprint, especially considering the rapid pace at which new technologies are being introduced. During this process, every bit of that data needs to be managed securely and compliantly, not only in stowage and transit, but also at the end of its lifecycle.

Company executives need to understand the importance of erasing data, they have legal obligations to destroy any sensitive information that is no longer being used. Not only do they have local hard drives and tape backups to contend with, but also mobile devices, memory cards and even virtual environments provided through the cloud.

Xperien CEO Wale Arewa says businesses exhibit a surprising degree of negligence when it comes to IT Asset Disposal (ITAD). "Not permanently erasing all data could be catastrophic for any organisation. In this age of smart interconnected technology, one needs to realise that every bit of electronic information is stored on a physical device somewhere - either on a hard drive, flash memory or tape."

Businesses need to keep track of data assets that have come to the end of their lifecycle and then destroy them at their origin. This might not sound too difficult, even for someone with basic knowledge of technology. After all, most people are familiar with concepts like a disk format and factory reset.

Unfortunately, secure data destruction is not that simple. Neither of the methods above guarantees that the information stored on those devices won't be recoverable. In fact, it will only take a few minutes with a free software package to retrieve it.

Arewa says most people assume hard drive format or a factory reset on a smartphone wipes the medium outright. "This is unfortunately far from the truth, a format or factory reset leaves almost all of the data intact. Its purpose is to strip out the existing file system and generate a new one, not to securely and permanently erase sensitive information. The user might not be able to access it as normal, but it's still there."

Destroying hardware is also no guarantee that the data will be unrecoverable.

Hard drives are easy to transfer from one machine to another. Even a shattered hard drive can be reassembled and transcribed with enough effort.

"Even taking a hammer to hard drives won't necessarily render sensitive information irretrievable. There's a need, for reasons of legality as well as privacy and security, for even securer techniques for the destruction of end-of-life data," he warns.

A backup tape is normally created to ensure business continuity, to keep the business running should access to live systems be lost. An archive is created for the long-term preservation of data and these tapes are often a crucial source of evidence to any investigation.

Arewa says companies need to find the best way to understand what data is vital or even legal to keep. "Businesses are increasingly seeking assistance in identifying the potentially relevant legacy tapes that have been kept in storage for the last 10 years, gathering dust and incurring substantial storage costs. It is certainly not unheard of to come across archived tapes that date back so far that the organisation no longer has the hardware or software to understand what data the tapes contain."

Having a good understanding of what data is held could help reduce the risk of legal exposure and could also reduce costs. Sensible data retention policies could help organisations balance their legal requirements to store particular data for certain timeframes, while destroying data that it is no longer required to keep or which no longer has value to the business.

"Partnering with a trusted expert to ensure you target only the most relevant tape sets – without the need to recreate the original environment they were backed up on – can ultimately save a lot of time and money, enabling the access and review of key data to happen quickly and efficiently," he concludes.

Businesses can achieve peace of mind that their sensitive information won't be coming back to haunt them after it's been deleted. There are various fail-safe data destruction methods which vary wildly in cost and come with their own particular advantages and disadvantages, but doing the job properly is often as time-consuming as any other method and requires no less rigour.

For more information or to schedule an asset disposal or data destruction project contact Xperien on (011) 462-8806 or visit www.xperien.com