

Data: It's not rubbish, but it is easily recycled!

By Derek Morgan, Head of Strategy, CKS Group plc.

In 1983, Stephen King wrote a short piece for Playboy called "Word Processor of the Gods". In this horror, a middle aged man comes into possession of a computer whose [insert] and [delete] keys have consequences in the real world. He uses the machine to delete the family he doesn't like and replace them with a new one.

In 2006, BBC News featured an in-house "expert", clad with suitably geeky safety goggles, maniacally proclaiming "Hit it with a hammer!" as he desperately tried to demonstrate how an end-user might finally destroy personal and commercial information stored in the hard drive, or virtual vault, within their computer. The real horror was etched across the watching faces of computer professionals across the country, as his advice was simply wrong!

Basically, mechanical processes don't do a very efficient job of disrupting magnetic media.

There may be psychological value in hammering the dickens out of the pesky inanimate, but there can be little satisfaction when the result remains the same – prosecution for negligence in records management associated with inadequate handling of business data; or, at a personal level, identity theft and fraud.

The Information Commissioner, who enforces the Data Protection Act says it will be tough on organisations with lax security procedures. "Companies have a duty to store personal information securely and delete it when it is no longer required" says Assistant Commissioner Phil Jones.

Executives are kept awake at night by horror stories about data that won't die.

Inappropriate perceptions of scale are part of the problem. We tend to see everything in human scale, and don't quite comprehend just how effective we have become at miniaturisation. On one hand we marvel at how we can now fit thousands of songs on a new iPod, whilst on the other we are blinded to the quantity of data that can be stored on a 2cm strip of hard disk. Neither shredding nor crushing hard drives does any electro-magnetic damage to the content. It just makes reconstruction a tad more tedious for the boys in lab coats. Tedious: but rewarding.

You need to protect your own interests, and your organisation's interests. To do that effectively, you will need more than a hammer.

In our experience, we believe that there are only two effective methods for data deletion. Used selectively, there should be no reason for sleepless nights or horror stories.

Either you can use a specialist software application to instruct the drive controller to overwrite stored data or you can use a SEAP approved electromagnetic degausser which randomly disrupts the media surface, rendering the contents meaningless.

In the case of mechanical failure of a hard drive, there is no option other than degaussing. Most reputable computer refurbishment operations should have access to such facilities. Unfortunately, the operations that really should have such facilities as standard are the new WEEE treatment facilities, but, despite the low cost of such devices, there are no such requirements on these companies. Even if there were, ICER research tends to suggest that upwards of 90% of all such waste is destined instead for treatment and reprocessing on the European mainland – where standards are often lower still and onward shipping to more exotic destinations is easy.

Degaussing provides an industrial and highly cost-effective solution to hard drive wiping on a large scale, but it isn't really suitable for use by end-users or small businesses. It is also not suitable where reuse is a high priority as there is a high chance that the degausser will destroy the drives mechanics and surface by magnetically pulling components out of alignment internally. In these cases, the software option is the only correct path.

The trick with software based data wiping is to find a credible product that is continually updated as drive technologies evolve. This is no mean feat. There are simply very few reliable candidates. We recommend Blancco.

The Blancco products address the hard drive controllers directly, bypassing the operating system that is typically designed to protect the user from their own mistakes (and thus moves or hides instead of deleting data). The use of their products is increasingly mandated for use across the critical military and financial sectors, and for good reason...

Glamorgan's computer forensic unit has put this to the test. This laboratory often works for GCHQ, the UK Government's top secret communications headquarters and carries out computer forensic work on behalf of the UK police. Within a random test batch of 100 drives bought from sources such as eBay, were 12 drives that had been wiped using Blancco.

"We could not recover anything. It became clear as we conducted the research that there was a set of drives that had been forensically wiped and when we came across them they began to be easily recognisable because all that was there were zeros. There was no file structure, no list of what had been there, there was nothing," said Dr Andrew Blyth, head of the unit.

Leaving drives blank is after all the point of what Blancco does. But you do need to be sure that it is being used consistently and used properly. After all there is a cost, and less scrupulous companies are always looking for shortcuts. These shortcuts put your business at significant risk if they reduce the effectiveness of the data wiping.

Increasingly, customers are demanding and getting an onsite data deletion service. This allows oversight and validation before the equipment leaves your premises and for highly sensitive industries, this opens the door to potential reuse and resale of the sanitised asset – which returns monetary value to the business.

Further, demand copies of the evidence. Each Blancco usage generates a transaction record which lists the serial number of the drive that has been processed. You should obtain copies of these as a defence against possible claims.

When it comes to your customer, patient, student or employee data... don't trust anyone – demand proof. It's the only way of avoiding a lead role in your very own horror story.

CKS WILL DELIVER BOTH PEACE OF MIND & HIGH RETURNS ON REDUNDANT ASSETS

The CKS Group specialises in secure asset recovery associated with changes in people, technology or business.

- Staff change – CIPD reports that the overall employee turnover rate for the UK is 18.3% and that the public sector has an average turnover rate of 13.3%.
- Computers change – Moore's Law has, for 40 years, successfully predicted a doubling in computing capability every two years - equating to an average performance improvement in the industry as a whole of over 1% per week.
- Businesses change – Barclays Bank reports in the past twelve months, a net increase of 60,000 in the number of firms in the UK – and a simultaneous 22.5% rise in business closures.

Unfortunately these events seldom align – as a result asset recovery is more about change management than it is about end-of-life disposition. Without an effective recovery partner, asset value is wasted and confidential business and personal data is exposed to risk.

Through the innovative application of best practice in redeployment, together with key security partners such as Blancco, CKS has served as the partner of choice for asset management firms like CSC and Getronics. We could say we are trusted, but we don't. Our customers freely conduct random checks and audits. You should too.

With CKS you don't need trust. You get proof.

For more information contact us on 01344 307 788 or visit us online at www.cksgroup.co.uk

CKS Group plc, a PLUS-quoted company, is a founder corporate member of the Institute of Information Security Practitioners, has facilities that are licensed with the Environment Agency, and has ISO:9001, ISO:14001 and IIP accreditations.