WEEE: must avoid data theft

For too long, people have simply dumped computers and other piece of hardware in bins, landfills and skips. There are the obvious hazardous material issues with this cavalier attitude and thankfully the European Waste Electrical and Electronic Equipment (WEEE) directive is addressing this.

It is disturbing to see the images from countries in Africa and certain areas of India and China where unscrupulous computer traders are dumping computer hardware to be recovered and recycled. These tasks are often carried out by children and expose them to a witches' brew of poisonous chemicals and fumes. The recovered metals and plastics are then recycled with no regard to the human cost. Part of the responsibility of any vendor of electronic equipment is to ensure that the device (or the one it is replacing) are recycled in accordance with all relevant legislation. This is critical for the safe and efficient handling of the components recovered but does not address the area of the information that may have been stored on these devices.

I have been horrified to read that as recently as twenty years ago paper based medical files were being tipped into a landfill in the south-west of the country and recent rail track laying activity uncovered them. This was a very unsettling time for people wondering if their personal, sensitive, medical information was on these files, and had anyone looked at them.

We should have the same fear with regard to the procedures organisations have for handling digital storage devices that contain our personal information. We should be asking questions of the organisation on their policy with regard to information erasure and destruction, records management and proof of data destruction for the relevant devices and proper asset management.

In 2007, Rits Pondera carried out an investigation as to whether people were deleting or destroying information on digital storage devices that were available for sale second hand in Ireland. The results were staggering. Rits Pondera acquired thirty hard drives from private sellers on www.eBay.ie and www.buyandsell.ie. Of these, 80 per cent were accessible and had information accessible on them. Of these disks, 33 per cent came from the corporate sector and the previous owner was easily identifiable.

Most of these had information on them that could have been used for identity theft from their customers, or financial fraud via credit card information. More than half had data on them that would have been in breach of the Copyright Act (copies of games, movies, CDs etc). Almost half of disks analysed had some form of pornography, although none would have been illegal. What these statistics for the Irish market show is a distinctly cavalier attitude from individuals as well as corporate entities to the erasure of information from devices that are being replaced.

Of the thirty disks that were analysed, some form of file deletion had been attempted, but this was not successful in any case. In the majority of cases, the use of a file un-delete utility would have recovered all files of interest. It would have been a trivial matter for anyone that acquired any of these disks to recover the information from them.

There are very strict regulations in place with regard to the safe and environmentally friendly handling of computer equipment under the WEEE directive, but there is no equivalent for the management of information on these devices. For example, an organisation that is handling sensitive personal or financial information may consider it appropriate to have all data erased from the medium in advance of the recycling partner removing the equipment from the customer premises. This sort of policy would apply to all digital media and ensure that the organisation would not be exposed to the risk of disclosing sensitive information.

It is also critically important to ensure that the tools being used for data destruction are appropriate for the task at hand, bearing in mind who the potential adversary may be, the value that may be assigned to the information and any legislative instruments that would govern the data. This issue also arises for organisations that may want to donate hardware for school project etc and for the donation to charities that are deploying them in the developing world.

Where a digital storage device is being disposed of or passed on to another organisation, the information on that device must be erased in a secure, non-re coverable manner. This is true whether it is a privately held or corporate device. There are many certified utilities on the internet and organisations offering support in the Irish market for these requirements.

Rits Pondera will be performing this audit of equipment available for sale in Ireland via www.eBay.ie and www.buyandsell.ie. It will be interesting to compare them to the 2007 results and, hopefully, comment on the improvement we are seeing in the Irish market. As we evolve into a more digital society, there are more and more fragments of information about us stored on systems everywhere. These range from our digital cameras and phones to retailer loyalty systems and onto financial and central government systems.

At every point where there is some portion of our digital identity stored, there is also the risk that this information is not managed or handled in an appropriate fashion. This includes the scenario where digital processing and storage equipment such as hard disks and backup media are transported and managed. It is this portion of the digital object lifecycle that we are interested in. Conor Flynn is technical director of Rits Information Security.

Rits Group Head Quarters
Information Security Centre
2052 Castle Drive
Citywest Business Campus
Co. Dublin
Ireland

Tel: +353 (0) 1 6420500
Fax: +353 (0) 1 4660468
Email: info@ritsgroup.com
Web: www.ritsgroup.com