Secure I.T.
DISPOSALS LIMITED

How to Choose a Secure Data Destruction Method

White Paper

By Andrew Speedie
August 09

Executive Summary

When dealing with end of life data there are a number of methods to ensure that the data is securely and permanently destroyed. This includes erasing, degaussing, shredding and disintegration. For each of these methods there are different methods, standards and processes, and numerous reasons for determining which method to use.

There are pros and cons for each destruction method and most organisations will use a combination of methods to comply with their internal policies and legal obligations.

Before a data destruction policy can be formulated two important questions have to be answered. Where the data stored is - hard drives, CD/DVD, USB sticks, mobile devices, etc. And what damage would occur if the data came into the public domain, i.e. what is the risk to the organisation if data is lost.

The method of destruction will depend on the risk. And the methods range from doing nothing (not a good idea), to a single pass erase, to shredding to MoD Top Secret levels. The choice will be determined on the risk of data loss and the balance between the cost and any resale value of the equipment.

Index

The Issues Surrounding End of Life Data

Until September 2007 there was little interest by most organisations in what happened to their data once it had reach the end of its life. It was only when the details of millions of people were lost by the Government and numerous other data losses that the security of data came to the fore.

During the life of a computer, a great deal of time, effort and money is spent ensuring that data is stored and processed securely, but too little attention is given to data when the computer becomes redundant.

When a computer becomes redundant it is almost certainly the time of greatest risk. It will be moved from pillar to post, handled by all and sundry and all the time it will still contain data.

Data Protection and Data Destruction

The legislation covering data protection is often overlooked, or worse, assumed that someone else will deal with it. This is rarely the case. For examples follow this link:-
http://www.ban.org/BANreports/10-24-05/documents/DataLeftonHardDrives.htm

Typing "data loss" into Google brings up hundreds of news stories, which demonstrates that, not only can it happen, it does. The cost to any organisation of losing data under these circumstances is incalculable

The main reason why data is not erased is time and money. The resources required (time and space) can be considerable and the cost to erase a disk can be as high as £10 per disk to guarantee data destruction to UK standards.

What standard should data be destroyed to? There are three main standards that are used, US DoD, German Din and the UK/MoD Approved standards.

The US and German standards are now over ten years old and have not been updated to take account of newer technologies, modern hard drives and tapes.

The Communications-Electronics Security Group (CESG), who carry out product approvals. Hold a number of approved products and a full list is available from www.cesg.gov.uk.As a minimum data should be erased to MoD Approved/CESG Baseline standard, this can be done using Kroll Ontrack Data Erasure, Ibas or Blancco.

If the data can not be erased using software then the disk needs to be degaussed and then shredded. Also using MoD Approved/CESG approved products and procedures.

There is one other standard for data destruction and this is your own. The risk of data loss can only be fully determined by the company that produces and owns the data. Sometimes this can mean not allowing any data to leave the site or using different data destruction methods for different types of data. Two tier standards such as these are normally only used by the MoD.

There are two methods that should never be replied upon. Reformatting the disk and assuming the data is not important and doesn't matter. Reformatting the disk does not remove the data and there are easily available tools that would allow an amateur to recover the data. It should never be assumed that data is not important. Every time a file is opened on a PC a temporary file is created, this includes Word documents, emails, web pages, etc. Over the life span of a PC 1000's of documents will be opened.

But just because your equipment is redundant to you, it doesn't mean that it has no value. On the contrary, most equipment does have some value and if there is a market for it, then it can be sold and, the revenue returned to you.

One of the key goals for many organisations is to see a return for their equipment. This is nearly always achievable if the equipment is disposed of in a timely manner. Unfortunately, many organisations keep the equipment far too long, worse still; it is kept in storage rather than the problem being tackled. It is estimated that redundant computer equipment kept in storage depreciates in value by 10% per month.

Legislation

The two main areas of legislation cover data protection and the environment. However the disposal of computer equipment is covered by over 8 separate regulations. These are: -

- Data Protection Act
- Environment Act
- WEEE Directive
- Hazardous Waste Regulations
- Landfill Regulations
- Electrical Equipment (Safety Regulations)
- Basal Convention, Trans Frontier Shipment of Waste
- Sarbanes-Oxley Act
- Sale of Goods Act
- Distance Selling Regulations

A brief outline of each of these regulations is given in Appendix A

Determining the Risk

Before you can decide the method of destruction the risk of data loss to the organisation has to be determined?

To aid this determination CESG has produced a useful document which details the risks and provides tables to categorise the impact levels, HMG Infosec Standard, Business Impact Table (Extract from Infosec Standard 1). This is a publicly available document downloadable from the CESG web site.

Briefly it details six impact levels 0-6. These range from Impact Level 0 where the loss of data will have no impact to the organisation and Impact Level 6 where the loss of data could lead to loss of life, the complete failure of the organisation, or cause the downfall of the Government

Examples are shown below

Impact	**Level**
No detectable impact	**0**
Cause losses of up to £1,000	**1**
Cause losses of up to £10,000 or threaten an SME	**2**
Cause losses of up to £1m or threaten a minor UK company	**3**
Cause losses of up to £10m or threaten a major UK company	**4**
Cause losses of up to £100m or threaten a major international company	**5**
Cause losses in excess of £100m or threaten the UK economy	**6**

HMG Infosec Standard, Business Impact Tables provides detailed information to cover all sectors of the UK economy and government organisations. Including public and private sectors, defence and government assets.

However these are just a guide. The organisation and the people responsible for data security have to determine the damage a data loss would cause to the organisation, individuals or the country.

For example the Business Impact Tables conclude that Impact Level (IL) 0 would cover the loss of data that had no, or a reliable impact on the organisation. But most organisations will determine that any loss of data is unacceptable. Not because of the financial cost, but because of the resultant negative publicity.

Is All Data the Same?

In a word – No

Within any organisation there will be numerous levels of data. Ranging from information already in the public domain, i.e. web site, through payroll information, to information that could cause the failure of the organisation, loss of life or threaten the stability of the country.

When preparing for a risk assessment, data is normally categorised into threat/damage or impact levels (IL). The example below is for a typical large national business

Impact Level	Category
0	Information already in the public domain, i.e. web site, public records
1	Information about employees not in the public domain, i.e. contact details
2	General internal information about the company not publicly available
3	Payroll, sales and customer information
4	Customer credit card details
5	Senior management remuneration, sales and cash flow forecasts
6	Bank login information, strategic and flotation plans

Most organisations believe it is best practice to treat all data to the highest level. This is acceptable if they believe that the costs involved with handling data to the highest level out ways the risk of a data loss. By handling data to the highest level the procedures, training and policy enforcement are significantly easier to implement.

A “one level fits all” policy is normally the easiest, and overall, the most economic to implement.

However for organisations that handle sensitive data, categorising their data and then ensuring that different categories are not mixed is fairly routine. Typically these are in the defence, intelligence agencies, NHS, Police and central government. By categorising data the cost involved with its life cycle and eventual destruction and be minimised.

Organisations that hold personal details on individuals need to ensure that this data is treated with special care. Not only do they have a duty of care to the individuals, the also have a legal obligation.

These types of organisations differ from normal companies in as much as they store data on individuals that could cause financial damage, or even injury or death to that individual.

These include:-

- Police Forces and Police Authorities
- NHS, SHA and PCT
- Banks and building societies
- Central Government Agencies, CSA, HMRC, etc
- Intelligent Agencies
- Defence Contractors
- MoD

Are All Organisations the Same?

In addition to determining the impact level that the data could have if it was lost and came into the public domain, the damage will vary depending on the type of organisation.

Small companies could suffer a data loss and nobody would notice, the press would have no interest and as long as they had backups the company would suffer no long term affects.

However the press would be very interested in larger companies, particularly any company that handles personal information such as banks. It would make little difference to the press if the data contained no useful information.

And every data loss by any public sector organisation will make the headlines regardless of the information concerned.

Only the organisation can determine what damage a data loss possesses. Some will conclude that they only need to use Impact Levels 0-4 (low risk), some will utilise all levels 0-6 and some will almost certainly only be able to consider Impact Levels 4-6 (high risk).

If the organisation chooses to pursue a one-size-fits-all policy then the method of destruction is a simple matter to deduce. If they categorise their data and determine they need a range of Impact Levels then a number of different data destruction techniques may be required.

Determining the Method of Destruction

Once the Impact Level or Levels have been determined then the data needs to destroyed. There are several methods of destroying data. These include erasure, degaussing, shredding and disintegration.

For each method there are various different levels of destruction. This allows for the particular destruction method to be tailored to the Impact Level.

Before a decision on a method of destruction can be made, the place where data is stored has to be determined. Some items are oblivious such as hard drives, CDs and USB memory sticks. But other are often over looked and have led to stories appearing on the BBC’s News web site
See http://news.bbc.co.uk/1/hi/technology/7635622.stm

Data, Data, where for art thou?

Data can, and is, stored in numerous places. Below is a list of most of the common pieces of equipment that hold data.

- Laptops
- PC Base Units
- Servers
- USB Sticks
- Memory Cards
- Digital Cameras
- Mobile Phones
- MP3 Players
- Disk Arrays
- Tape Drive (quite often a tape is left in)
- Routers
- Switches
- Printers
- Copies
- Faxes
- Multi Function Devices (MFD)
- PDA's
- CDs
- DVDs
- Tapes
- Floppy Disks
- CCTV Tapes
- Digital Video Recorders (DVR)
- Smart Cards
- Mobile Phones and their SIM Cards

In addition when most printers are disposed of they still have company letterhead paper in the paper trays, or even medical prescriptions.

Laptop bags are another source of personal information. The have so many accessory pockets that something normally get lefts behind.

Which Data Destruction Method to Use

All data can be removed from any device or media and that item can then be resold or reused. Sometimes the cost of removing the data out weighs the return and in this case the only option is physical destruction.

But why physically destroy an item, why not erase or degauss it. The answer isn't a simple one and a number of facts have to be considered.

- Number of items requiring data destruction
- Type of item
- Impact Level
- Cost

For example:- You have 200 hard drives that have low level data. These could be erased, but for a typical 10 GB disk taking 6 hours that's a long time. And there will be a cost for erasing each disk.

They could be degaussed, and using CESG approved degaussers this is reasonably quick and inexpensive. However there is no visible physical change to the item and the process damages the electronics making verification impossible and therefore data recovery a possibility. In addition, degaussers only erase data on magnetic media. This still leaves, memory cards, mobiles, CD, routers, PDA's: in fact most media and devices that store data.

Physical destruction does have a high initial daily cost. But it will destroy all types of devices and media and once certain quantity thresholds have been reached the cost is comparable with both erasing and degaussing. It is also significantly quicker than erasing and guarantees 100% that data can not be recovered.

So why not just shred everything?

Once an item has been shredded there is no possibility for reuse. Even with degaussing it is only tapes and floppies that can be reused. And then not the latest LTO, DLT's, etc. The process removes the control tracks.

A good example of where erasing is the only viable method is where the item has a high resale value, is leased or is going to be redeployed either elsewhere in the organisation, or externally, i.e. a charity donation for instance.

Data Erasing

Data erasure* is performed using **UK/MoD CESG/MoD** Approved standards equipment and procedures, and then shredding if not for re-use/return.

HMG IS5 covers both baseline and Enhanced overwriting of data. At 'baseline' level the software overwrites every sector of the Hard disk with one pass of randomly generated data. At 'enhanced' level every sector is over-written three times: first with a 1, then every sector is over-written again with a 0, and then every sector is over-written a third time with randomly generated 1s and 0s. whether baseline or enhanced methods are used a verification pass should always be applied.

*If a hard disk is faulty and cannot be erased then it should be physically destroyed by using an industrial shredder.

Degaussing

Erasure via degaussing may be accomplished in two ways: in AC erasure, the medium is degaussed by applying an alternating field that is reduced in amplitude over time from an initial high value (i.e., AC powered); in DC erasure, the medium is saturated by applying a unidirectional field (i.e., DC powered or by employing a permanent magnet).

Shredding/Disintegration

The shredding/disintegration process utilises a purpose built Low speed, high torque, industrial disintegrator, which involves a process of cutting and grinding the medium into small particles that are finally reduced to pass through a screen (40mm - 6mm dependent on security requirements). At 6mm not even the world's most capable IT professionals could piece the data together again.

Conclusion

Generally there is no one perfect solution to computer disposal. And almost certainly a combination of one or two methods will be deployed.

These days financial, stakeholder obligations, CSR and legal compliance are the main driving factors behind how computer disposal policies are defined and by using a Specialist Disposal Partner all of these concerns can easy be addressed. If a Trickle down Policy is also employed then a balance can be achieved in maximising the life of the equipment and ensuring legal compliance at minimal costs.

The advantages for using a specialist recycling partner is that they will assume liability from when they collect the equipment. And as long as a reputable, fully licensed partner is chosen then they will be erasing data to CESG standards and will ensure that any equipment that requires recycling is processed in accordance with all UK, EU and international laws.

A specialist recycling partner will also be expert at maximising the return for remarketable equipment and will be able to provide a return for your equipment or at the very least keep costs to a minimum.

About the Author

Andrew Speedie has been involved in secure data destruction for over 20 years and is highly qualified in the area with both a BSc Hon's in Computer Science & Software Engineering and a HND in Electronic & Electrical Engineering. He is the security controller for Secure I.T. Disposals Ltd.

In 1990 he established Speedie Computer Systems and brought computer scrap from ICL, (now Fujitsu) destroying the data, refurbishing and reselling it. From the first collection it was apparent that the data would have to be removed from all drives, and so the US DoD data erasure standard was adopted. The US DoD standard was used until 2003 when the CESG standards were published

In 2003 following a de-merger, Secure I.T. Disposals Ltd was formed and still incorporates Speedie Computer Systems as the retail sales division.
Shortly afterwards Secure I.T. Disposals achieved BSi accreditation for ISO 9001, ISO 14001 and ISO 27001. The following year they were awarded Investors in People status.

As part of his role as Technical Director, Andrew has been actively involved with consultation with the Environment Agency, Defra and ICER regarding the implementation of the WEEE Directive. CESG have also consulted with him regarding changes to the data erasure standards.

Andrew is always willing to advise on matters regarding data destruction and the recycling of computer equipment.

Further details can be found at www.sitd.co.uk

Appendix A

Data Protection Act

Under the Data Protection Act anyone who processes personal data has to be registered with the Information Commissioner and has a Duty of Care to ensure that all data is not kept for any longer than necessary and is properly destroyed when it is no longer required

Environment Act

Under the Environment Act waste is defined as anything that is redundant to an organisation or that an organisation needs to dispose of. All waste must be disposed of using a fully licensed waste management site and transported using a licensed waste carrier. The Act also defines your Duty of Care and this extends to when the equipment is finally disposed, reused or recycled.

WEEE Directive

These regulations cover the recycling of waste electronic and electrical equipment. The aim of the directive is to place the burden of the cost of recycling with the manufacture or importer and they have to pay for the recycling of all consumer WEEE. They also have to provide a recycling service for business customers, but can charge for this service. They also have no obligations regarding data destruction. The cost is subject to negotiation.

The WEEE Directive is due to come into force in July 2007.

Hazardous Waste Regulations

From July 2005 these regulations were incorporated into UK law with the proposal of bringing the UK in line with current European waste classification. Under these regulations CRT monitors and UPS are now classed as hazardous waste and as such any organisation disposing of over 200kgs (approx. 15 monitors) have to register with the Environment Agency as a Producer of Hazardous Waste. Only an Environment Agency licensed waste site can dispose of the equipment.

Landfill Regulations

These regulations severely reduced the type of waste landfill sites can accept, reducing the number of sites that can take I.T. equipment from nearly 300 to around 12. This followed the reclassification of waste under the Hazardous Waste Regulations

Electrical Equipment (Safety Regulations)

As implied these regulations cover electrical safety and state that the owner/supplier of any electrical equipment must ensure that it is electrically safe. It particularly mentions testing following the movement of equipment, since this is when there is most likely to be a failure. Testing is carried out using Portable Appliance Testers (PAT) and should be carried out every 12/24 months, and, after the equipment has been moved.

Basal Convention, Trans Frontier Shipment of Waste

This convention is signed by members of the OECD, the EU and a few other countries and as such is incorporated into UK law. The convention specifically prohibits the export of non-working and untested electrical and electronic equipment to any country that is not a member of the OECD or the EU. The Convention classifies waste into three categories, Green, Amber and Red

- Green List covers PC, laptops and printers etc

- Amber List covers CRT monitors, UPS, bulk batteries, etc
- Red List covers reactive chemicals, explosives, etc

Any export of non-working or untested equipment from the UK to EU is governed by the Trans Frontier Shipment of Waste Regulations and requires a TFS route be established for Amber and Red list equipment. This involves paying the Environment Agency vast sums of money in TFS fees and Bonds.

The main driving factor behind this Convention is to stop the dumping of waste into countries that do not have the facilities or legislation enforcement to deal with the waste in an environmental friendly way.

The trade in non-working and untested monitors to Africa, India, Pakistan, China, etc is huge and the affects on the local environment is catastrophic. Type "export of electronic waste" into Google or visit the Basal Action Network at www.ban.org.

Sarbanes-Oxley Act

In the United States, the Sarbanes-Oxley Act makes corporate executives explicitly responsible for establishing, evaluating and monitoring the effectiveness of internal control over financial reporting. For most organisations, the role of I.T. will be crucial to achieving these objectives. The main concerns regarding I.T. is auditing to systems and data lifecycle management, including ensuring data destruction.

Whilst this is a United States Act, many UK companies that are have a presents in the US are covered by it and should be taking steps to ensure compliance.

Sale of Goods Act

The Sale of Goods Act states that equipment must be fit for purpose and must remain fit for purpose for a reasonable period of time. For refurbished computer equipment this means providing a warranty of between 3 and 12 months.

Distance Selling Regulations

These regulations allow customers to return any item for any reason with in a reasonable period of time. The customer is entitled to a refund of the purchase price, less a restocking fee is applicable.