ADISA

APRIL 2012 ISSUE 1

IT ASSET DISPOSAL • RISK MANAGEMENT • COMPLIANCE • IT SECURITY • DATA PROTECTION

Exploring the challenge of erasing solid state media

Page 6

Information Commissioner's Office gives an insight into how they view the area of IT asset disposal

Page 9

Welcome

to the first edition of the ADISA magazine, the only publication dedicated to the issues surrounding IT asset disposal (ITAD).

Launched in 2010, ADISA is raising awareness of the data protection risk within the asset disposal process and working with all parties to help reduce that risk; improve service quality; raise professionalism; and promote re-use within the IT disposal channel.

ADISA defines IT asset disposal as:

> **Any situation where the data controller transfers custody of an IT asset to a third party for management or processing whether on a temporary or permanent basis**

Asset disposal is viewed by many companies as only occurring at end-of-life. However, other activities including end-of-lease or a break / fix scenario must be considered. Furthermore, if any organisation is using the cloud or a hosted data centre provider then assurance about sanitisation of data from those service providers must also be sought.

In 2011 ADISA launched the first dedicated standard for IT asset disposal service providers. At the time of going to press, 16 UK companies have passed the standard and there are over 20 working towards certification. Further audits are booked in France, the US, Canada and Australia for 2012 so the standard is beginning to get widespread adoption. This standard is being used as a prerequisite by many companies seeking IT asset disposal service providers as it shows that potential suppliers have passed an exacting audit process.

With the launch of this magazine, ADISA is providing industry service providers and data controllers a publication which will help educate on the issues of the day, provide ongoing advice on what is current best practice and keep the reader abreast of any changes which impact on the marketplace.

The magazine will evolve over time so content and ideas are welcomed for submission from all participants and can be mailed to submissions@adisa.org.uk.

Yours sincerely,

John Sutton and Steve Mellings
Founders, ADISA

Contents

Content Editors
John Sutton
Steve Mellings

Copy Editors
Simeon de la Torre

Content Authors
Wendy Davies
Gerry Masters
Dr Phil Turner
Alastair Barter
Simon Brailsford

Contributors
Rob Smith - SWEEEP
Professor Andrew Blyth – University of Glamorgan
Kyle Marks – Retire IT

Design
Tom Ovens
Nick Kelly

Production
Wei Kee

Advertising enquiries
Chris Godfrey
magazine@adisa.org.uk

Content enquiries
Steve Mellings
magazine@adisa.org.uk

ADISA
Hamilton House,
1 Temple Avenue,
London,
EC4Y 0HA
Tel: +44 (0) 845 833 1600

Secure erasure of solid state media – the challenges

by Gerry Masters

Perhaps more than ever before, IT users wield significant influence over the design stage of product development. Certain companies have led the way with technology which is not only functional but also aesthetically pleasing. This has not only led to a spate of copycat design issues but has also seen standardisation on specific user driven technologies such as touch screen and the adoption of smart phone and tablets as business tools.

For data storage, the use of solid state media is now widespread due to the quick access time and small form factor, which lends itself well for use in smart phone and tablet design. This technology is now creeping significantly into the netbook and laptop marketplace and as such the question of secure erasure is beginning to be raised in information security circles.

Gerry Masters, an IT forensic specialist, explores the challenges of erasure on solid state devices (SSD).

The ability to securely erase (sanitise) information from storage media is vital to maintaining the confidentiality of that information. It is crucial when writing about approaches to sanitisation that the media type is first understood. For SSD traditional overwriting techniques that work predictably for magnetic hard disk drives (HDDs) may not work so well and the reasons why are not understood, leading many policies and procedures to be simply not fit for purpose.

A technical comparison of HDD and SSD

The internal architecture and data management processes within an SSD are very different by comparison with a magnetic hard disk drive (HDD) and in summary the main differences are:

- An HDD consists of physical moving parts of which data is stored on one or more platters which spin to allow read /write to occur using fixed magnetic heads.
- An SSD is a fixed technology with no moving parts which uses a series of microchips (collectively called the Flash Translation Layer or FTL) to store and control access to the data.

An HDD works by reading or writing patterns of aligned magnetic fields in fixed locations on a rotating magnetic platter.

These locations, or blocks, are referenced using an internal physical address system. When a specific block (sector) needs to be accessed, its logical block address (LBA) is mathematically translated to a physical address in a predictable manner. A sector is the smallest storage area addressable on an HDD. Sector data is overwritten in-place at the specified LBA.

Figure 1 illustrates the origin of physical addressing.

Using the editing of a document as an example, if just one character is changed and the document is then saved, the disk is overwritten at a sector or cluster (group of sectors) level.

Occasionally, a sector will cease storing data correctly. When this occurs, the disk controller electronics will record the physical address of the 'bad' sector and will redirect any LBA requests to access the sector to a pool of spare sectors (this is known as sector reallocation).

An SSD works by storing data in one or more flash memory chips.

Figure 2 shows a 2.5" form factor SSD with the cover removed.

The memory chips are divided into 'pages', 'blocks' and 'banks'. A block contains a number of pages and a bank contains a number of blocks. In the case where an SSD contains more than one memory chip, an added complication is the 'mix'. The mix is a process of writing data across multiple memory chips and can be at either page, block or bank level.

HDD v SSD

SSDs have a number of advantages over HDDs: they have no moving parts (noiseless and more robust); data access is faster; consume less power and are not affected by magnetic fields.

SSDs do, however, have two major disadvantages: the data retention lifetime is typically only about 10 years and the memory cells have a limited number of re-write cycles – typically 5,000 to 100,000 – depending on the manufacturer. This limitation is known as 'endurance'.

To improve a device's endurance a wear-levelling process (algorithm) is used which prevents data being continually written to the same location. The algorithm used varies depending upon the manufacturer of the device controller and the storage capacity.

The device controller uses a flash translation layer to manage the mapping between LBAs and the pages of flash memory. This mapping has the effect of scattering data across the device.

Further autonomous movement of data is caused by internal 'garbage collection' processes when a device is powered up.

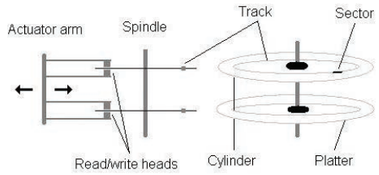

Figure 1: Schematic of an HDD

Definitive information about what these processes actually do is extremely scarce and is outside the scope of this article.

Each block of memory normally includes a small area that is used to store its sequence number, error checksums and markers to indicate if a page is active.

Additionally, because memory cells have limited endurance and will eventually fail, the SSD controller has the ability to mark a particular block as failed (inactive) and re-map that particular block. Using the editing of a document again as an example; if just one character is changed and the document is then saved, the device is overwritten at block level.

The problems associated with the sanitisation of SSDs

Degraded cells

Should a cell reach its maximum number of read/write operations, or fail for another reason, the FTL will denote it as inaccessible (degraded). Consequently, the FTL will not allow any subsequent data wiping operation access to the degraded cells. Therefore, the user data stored in the degraded cells will remain un-sanitised.

Wear levelling

Due to the action of the FTL an in-place overwrite of the sector at the LBA level is not possible. To re-write a sector, the FTL will write the new contents of the sector to another location and the map is updated accordingly with the translated LBA location. Consequently, the old version of the data will remain in its original location.

Device capacity

Device capacity can be up to 25% greater than stated on the label, or reported by software.

Unlike an HDD, an SSD does not report the number of reallocated pages, or the full physical capacity of the device; hence the user or erasure software cannot report or erase the entire physical device.

Physical destruction

Considering the physical destruction aspect, modern memory chips store huge amounts of data in a relatively small volume of material. Therefore, the current practice of grinding them to, for example, 2mm pieces may be ineffective, because the encapsulated silicon component may not be fragmented by such processes.

Conclusions

In the light of the issues raised, the following conclusions have been drawn:

- In-place sector updates are not possible in SSDs; hence the overwrite-based erasure techniques that work satisfactorily for HDDs are invalid for SSDs
- The true physical capacity of a device can only be determined by dismantling it and examining the memory chip(s) contained within
- If the number of reallocated pages is not reported, then the erasure product cannot properly overwrite an entire device
- Physically grinding chips into small pieces to destroy the data is not reliable when faced with technically advanced threat adversaries

So, how to sanitise SSD?

The conclusions indicate that the following questions, as a minimum, should be asked of the vendor of the chosen erasure product, or the data destruction service provider:

Does the product correctly report the true full physical capacity of the device to be erased prior to the erasure process?

This can usually only be verified by dismantling the device to determine the capacity of the memory chips that are used. If the capacity is correctly reported then the product is likely to properly overwrite the entire device.

Is the product capable of accessing all physically addressable areas of the device and not just the logical capacity?

If it is capable, then the erasure process is likely to properly overwrite the entire device.

In the case of physical destruction by grinding, what process is used to verify that the fragment size is appropriate for the memory devices within the SSD?

The current practice of grinding to 2mm is based upon the memory technology available at the time of production of the relevant standards. However, technology has moved on and the present consensus suggests that a fragment size of 0.5mm would be more appropriate. Furthermore, within a few years, that figure may realistically be closer to 0.2mm – which is effectively a coarse powder.

Reference to the memory chip manufacturer's documentation, if available, may be the only method of verifying that the fragment size is appropriate in any given situation.

Editors comment:

The appropriate destruction process for SSD must be underpinned by an agreed risk analysis, which determines the sensitivity of the data and the motivation and capability of any type of threat agent or attacker. Some of the vulnerabilities which are exposed by Gerry's technical assessment of SSD sanitisation are clear for all to see but in some instances only the highly trained and well-resourced threat actors are capable of undertaking the level of attack where data could be recovered. Each data controller should be aware of these challenges and make their own assessment of an allowable process for sanitisation commensurate to their own requirements.

Recommended further reading

1. Reliably Erasing Data from Flash-Based Solid State Drives: Michael Wei, Laura M. Grupp, Frederick E. Spada, Steven Swanson, University of California, San Diego, USA.
2. Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? : Graeme B. Bell and Richard Boddington, The Journal of Digital Forensics, Security and Law, Volume 5, Number 3, 2010.

About the author:

Gerry Masters was formerly part of the QinetiQ digital forensic and data recovery team and has recently founded Digital Infosec Ltd. He can be contacted through the magazine press office or directly at info@digitalinfosec.co.uk.

Associate author:

Dr. Phil Turner was also formerly part of the QinetiQ digital forensic and data recovery team. He can be contacted at philip.turner@hp.com.

Figure 2: A 2.5" form factor SSD containing multiple flash memory chips

ADISA

INTRODUCING
ADISA IT ASSET DISPOSAL STANDARD

IT Asset Disposal is a largely unregulated and highly competitive service sector. With over 650 IT disposal companies in the UK alone, it is difficult for organisations to understand who to use and who to trust when disposing of IT assets. A cursory search on the internet will show a myriad of different companies all seemingly offering the same service utilising the same "approved" tools.

So who do you use? Who do you trust? The ADISA standard has the answer for you.

Launched into the UK in 2011, the ADISA ITAD standard has been widely adopted by the leading companies in the IT disposal industry. Certified companies understand the necessary elements which make IT disposal secure and are able to demonstrate this with compliance against the ITAD standard. With 16 sites already certified this standard is quickly becoming THE certification your disposal suppliers should hold to show their quality of service.

ADISA STANDARD KEY ELEMENTS

- Business Credentials.
- Risk Management during logistics
- Creation and maintenance of the chain of custody.
- Physical security of the asset throughout the process.
- Promotion of re-use wherever possible.
- Quality controls.
- Using approved tools for each media type.
- Technical competence.
- Segregation maintained at each stage.
- Downstream supplier management.

THE AUDIT PROCESS

- Independent auditing from SGS (www.sgs.com)
- Full pre-audit assessment of written documentation.
- Annual audit to ensure that compliance with the standard is maintained.
- Spot check audits throughout the year to maintain integrity.

BENEFITS TO CUSTOMER

- Confidence that your supplier has been independently assessed and displayed competence throughout their process.
- Reassurance that your supplier is under constant scrutiny.
- Ability to make a sourcing decision starting from a small supplier base.

VISIT WWW.ADISA.ORG.UK AND SEE IF YOUR SUPPLIERS ARE ADISA CERTIFIED.

For further information please contact ADISA today on 0207 489 2008 or info@adisa.org.uk

The Information Commissioner's Office perspective on IT asset disposal

Alastair Barter, Senior Policy Officer for the Information Commissioner's Office reveals what the ICO looks for from a data controller during IT asset disposal.

When choosing a company to destroy personal data for you, it's crucial to ensure they are hot on security – especially because you, as the data controller, remain responsible if anything goes wrong. Alastair Barter, Senior Policy Officer at the Information Commissioner's Office, explains how to stay on the right side of data protection principles.

If your organisation processes personal data, you are responsible for doing so at every stage in line with the Data Protection Act 1998. The Act defines processing as covering almost anything you do with the data including collecting, storing, modifying and – just as important – destroying it.

The Act requires you to take appropriate technical and organisational measures to protect personal information – whether you (the data controller) or a third party (such as an asset destruction company) does the processing.

You retain liability for the information as well as full control over its use. The processor should only use the data in line with your instructions.

Your liability highlights the importance of choosing your destruction company carefully. You are responsible under the Act for what the company does with the personal information contained on old or decommissioned electronic devices.

So, if you're a prudent data controller you'll want to pick a company you believe can carry out processing securely. The first step is to get suitable guarantees about its ability to ensure security. But the Act requires other measures too.

You should have a written contract with the destruction company. It should make clear that they will only use personal data in line with your instructions. The contract should specify that data must be securely deleted before the electronic devices on which it is stored are destroyed or recycled. The contract should also say that the destruction company must take appropriate security measures to safeguard the data.

A contract allows you to keep control over the processing. This matters because if data is compromised in a security breach, you remain responsible. You can take further measures by auditing the company and requiring them to report security breaches or other problems when they occur.

Above all, you should be satisfied that you know who is doing what with the data you're liable for, even though you may no longer need it. You'll lack this assurance if you let a destruction company take devices away without forming a tight contract with them and verifying they are suitable. A breach of data security could result in regulatory action.

The Information Commissioner's Office is the regulator for the Act. In cases of serious non-compliance, we may impose a penalty of up to half a million pounds. Reasons for this could include failing to have a sufficient contract in place with a destruction company.

You should consider asking the company to tell you about any specific software or hardware they use when wiping or destroying drives. You can then do more detailed research about these products before deciding whether to go ahead with the contract.

You should be able to show you have completed a thorough risk assessment before engaging a third party to do this sort of work. You should also ensure there are comprehensive audit trails so that you can account for the equipment and its contents at all times.

Advances in technology may mean you need to periodically re-examine current contracts, along with the processes used by destruction companies, to ensure they continue to meet industry standards.

So you have a responsibility to ensure that personal data is secure at all stages of processing, including during destruction. For their part, destruction companies can help you comply by making it simple for you to understand what they offer, by knowing that a contract should be in place, and by giving a secure and reliable service.

A glimpse into the future of data protection emphasises how important it is for data processors, including destruction companies, to protect personal data. European Commission proposals suggest that in future more legal responsibility will fall on data processors. This could make them subject to regulatory action. It's a proposal that all destruction companies should keep an eye on.

Tier 1 Asset Management Ltd; 15 years and £50 million later...

Jonathan Rose: Tier 1 has given over £50 million back to corporate clients

It is a fact that corporate and government users of IT equipment – and more pertinently those who are tasked with disposing of it – are faced with a wider range of choice of supplier than ever before.

Whilst such an abundance of alternatives can sometimes be a good thing, we at Tier 1 Asset Management Ltd fully support the ADISA ethos that a discerning selection of premium quality, appropriately accredited specialists should be the only option for business IT users.

But how do businesses differentiate between these leading players in the ITAD industry?

If measurement is through longevity, independence and a successful track record of innovation and providing stress-free, secure IT disposal services, Tier 1 Asset Management Ltd should be an automatic choice.

2012 sees Tier 1 Asset Management Ltd celebrating fifteen years of providing dedicated secure IT asset management and disposal services to UK plc. Independent and unfettered to any IT suppliers and manufacturers, yet comfortably close to the leading lights in these sectors, Tier 1 handles some of the UK's largest and most sought after IT disposal projects.

In that time, Tier 1 has returned over £50 million of revenue to corporate clients.

Perhaps more astonishing is the fact that this figure has been achieved despite the price of new equipment plummeting to record lows, forcing the price of second user equipment down year after year.

Managing Director Jonathan Rose, an ADISA Advisory Council member, put these revenue return figures into perspective: "For the last few years as prices of new equipment have come down, we have been effectively running to stand still in terms of the revenue that we return back to our clients, particularly with a re-marketing model that focuses on direct sales to end users.

> **Tier 1 has a successful track record of raising standards through our emphasis on innovation and there's no reason why this shouldn't be any different in the next 15 years**

Fortunately, we have invested wisely in new online e-commerce technology and have been able to develop our B2B product sales model in order to keep returning industry-leading levels of revenue return to our clients. The year on year increase in the number of assets that we handle on behalf of a growing list of clients show how much we are trusted."
Whilst Rose admits that in these times of austerity, revenue return is attractive to Tier 1's corporate clients, the issue of data security is still the number one priority for British organisations. "We have managed to combine guaranteed data security and re-use of assets in their original form at a time when the market has veered towards a trend of physical destruction of assets. Our view is that the two are not mutually exclusive and the emphasis on re-use allows us to combine sustainability and revenue return with guaranteed information security.

The future will see Tier 1 continue to innovate in order to lead the ITAD industry and Jonathan Rose is optimistic that wherever our industry finds itself in the forthcoming years, Tier 1 will undoubtedly have paved the way to higher standards and advances in the disposal process.
"The one certainty in our sector is that businesses will always have equipment that reaches the end of its life and the disposal process will be connected to both data security issues and complex legislation. Tier 1 has a successful track record of raising standards through our emphasis on innovation and there's no reason why this shouldn't be any different in the next 15 years."

Developing and implementing an intelligent asset disposal policy

by John Sutton

It is the experience of ADISA that end-of-life decisions for IT assets are typically an afterthought, and often based on naive interpretations of a corporate asset disposal policy. ADISA also often encounters the complete absence of an IT asset policy, which may lead to serious data breaches, illegal IT waste export practices and missed opportunities for cost-recovery through sustainability programmes.

This article introduces the essential steps that lead to an effective asset disposal policy, which is based on commercial best practice and takes account of data security, environmental legislation and sustainability advantages. Additionally, ADISA advocates this policy must be underpinned by sound risk-based decisions that enable data/asset owners to make informed decisions about the choice of IT asset disposal (ITAD) service-provider; the most appropriate disposal method that balances security, environmental and cost-recovery considerations.

How to create an intelligent IT asset disposal policy

It is vital that this policy is part of an overall information assurance policy. It must not be created in isolation of other corporate information security policies, and wherever possible it is advisable to use the same risk-based approach used in the drafting of these other corporate security policies.

ADISA believes there are five crucial steps leading to the creation of an intelligent IT asset policy. Whilst all of these steps can be carried out within an organisation, particularly the first two steps, ADISA experience suggests that organisations often benefit from the assistance of external specialists.

Step 1 - Data categorisation

Organisations, irrespective of size or nature must absolutely understand the sensitivity and confidentiality of their own data. The end result of this step is a hierarchy of data confidentialities, which for example could be a simple UNCLASSIFED, SENSITIVE and SECRET model. Organisations must also understand how their clients, customers and partners have categorised their own data, and be mindful of appropriate legislation (e.g. Data Protection Act). The process for determining such a hierarchy of data confidentialities is discussed elsewhere in this publication.

Step 2 - Business impact tables

The purpose of this second step is to determine and quantify the potential impact on the business should any of the data (discussed at step 1) become compromised. The impact on the organisation can be quantified in terms of financial loss, reputational damage, client/customer confidence, litigation issues etc. There will be an impact statement for each of the data confidentiality levels established in step 1.

Step 3 - Threat profiling

This step involves making judgements on who is most likely to exploit and benefit from security breaches of an organisation's data. The first stage of the analysis focuses on those who would benefit (the threat source) from any data security breaches. Examples of these beneficiaries are rival business organisations, investigative journalists and organised crime. The analysis quantifies the motivation and priority of these potential beneficiaries.

The second stage involves analysing the opportunity and capability of those who actually attempt to exploit (threat agents) any vulnerabilities or weaknesses in the asset disposal chain. The two stages are then quantified within an overall threat hierarchy. Typically, this threat is then expressed on a 'very low' to a 'very high' basis.

Step 4 - Risk analysis

The previous steps are all inputs into step 4. A table of risks is determined by mapping together the business impact levels with the threat levels, which produces a hierarchical range of risk levels. It is only at this stage that the actual disposal process can be determined. For example, if the risk is relatively low and the corporate policy is to support sustainability (by reusing whenever possible), then this would rule out destruction options (e.g. shredding) and promote the use of a cost-effective data wiping option. However, if the resultant risk level is unacceptably high then a physical destruction may well be the only sensible option. The point being that whatever disposal process is chosen, it has been based on an intelligent risk-based analysis.

Step 5 - Selection of asset disposal process/procedure

This final step is to determine the actual disposal process or procedure. The inputs to any judgements made at this stage are the range of risks (from step 4) and the overall corporate policy drivers (security concerns, environmental issues and potential cost recovery/resale value). The processes that support sustainability are various data wiping utilities that will have differing cost and licensing arrangements. The risk levels will help the selection here. If physical destruction is to be the disposal process then shredding options would include the actual shred size to utter destruction by incineration. Again, the resultant risk levels will help in the selection of a suitable physical destruction process.

A table of corporate approved destruction processes mapped against the risk levels (determined at step 4) would be very beneficial to an organisation when selecting a service-provider (ITAD) to carry out the disposal of IT assets at end-of-life.

This overview of the steps leading to developing and implementing an intelligent IT asset disposal provides an introduction to the series of articles that will appear in future issues of this publication. The first article in this series can be found on Page 19.

Why data controller hardware asset management needs to extend into the disposal channel

by Wendy Davies, Managing Director of EOL

- Would you know if you lost an asset within your disposal process?
- Do you know if all the equipment shipped from your premises has been received and has undergone the approved data sanitisation process?
- Do you simply trust your partners audit process to update your own asset registers?
- How do you know if you've received all the revenue from the items released for disposal?

IT asset management (ITAM) is a widely established and respected data controller activity, however it appears that the remit of ITAM stops at the point of decommission, as many companies have very little control over their assets after releasing them into the IT disposal channel.

In the 2010 ADISA survey less than 5% of ITADs confirmed that their clients provided a full inventory when arranging a collection. In fact, the 2012 ADISA standard has been required to amend its criteria for client engagement, as the expectation on the ITAD was too difficult for them to adhere to simply because clients would not behave in a manner which would allow them to do so.

A casual straw poll of ITADs show that collection requests are often made as follows; "Can you please come in ASAP as we have a room full of equipment", "I don't know what we've got but it's about a van load" and "Just take these extra items please".

This type of uncontrolled activity may allow for operational flexibility but what happens if something goes wrong? Would any investigation actually be able to prove that assets were released and received for disposal? Would we be able to identify exactly where the assets were when they went missing?

What is the chain of custody within the IT asset disposal (ITAD) channel?

Whether the ITAD work is carried out onsite or allowed offsite there is usually a pre-determined point when hardware assets are passed from the responsibility of the data controller into the care and control of their chosen partner. From this point of transfer the ITAD will report back to the data controller on a range of activities which take place on the asset.

These will include:

- Verification of inventory received at the processing facility
- Confirmation of build and specification of devices
- Proof of data sanitisation
- Revenue realisation
- Recycling

This information will generally be delivered back to the client via an audit report, providing the client with a hardware asset "chain of custody" within the disposal process that can be utilised for a number of purposes:-

- Security verification
- Compliance evidence
- Inventory updates
- Software license management
- Resale value

Should there be loss of control over the assets at any point, the whole audit process is compromised, due to an inability to fully verify that all assets have indeed been passed through the hands of all participants and therefore received the intended services required.

Why is the chain of custody important?

For any organisation which takes its data protection responsibility seriously, and which wants to operate policies which are both ethical and environmentally responsible, then within IT asset disposal the importance of the chain of custody can be illustrated by asking these three simple questions:

1. Without a complete verifiable chain of custody how do you know that all data has been sanitised if you don't know what equipment entered the disposal channel?
2. How do you know that your disposal supplier is recycling equipment you designate as WEEE correctly and is not wilfully brokering YOUR waste equipment or shipping it abroad when you don't have any initial inventory to check against?
3. How can you audit your suppliers to ensure that you have accounted for all your assets and know where they ended up?

Asset loss can, and often does, occur within the data controller's own organisation, potentially during logistics or during the processing aspect of disposal. Without control over the assets which allows for verification and clear boundaries of operational and/or legal responsibilities, should anything untoward occur then there can be no evidence of genuine due diligence and any investigation is hampered by a lack of audit trail.

Conclusion

The whole area of "disposal" is something many companies simply underestimate as a source of potential non-compliance, and as such do not place a particularly high importance on it. At some point, every organisation must accept their responsibilities within disposal and confront the challenges within it. One of those key challenges is that of a verifiable hardware audit trail throughout. This can only be achieved by the creation and management of the chain of custody from point of decommission through data sanitisation ending with resale or recycling of the asset. A failure to grasp this will leave organisations wide open to the loss of assets, which exposes potential data breach, loss of revenue, embarrassing press or adding to the ongoing e-waste problems in the developing world.

Spotlight on...

Simon Brailsford, Director of Sales at Greenworld Electronics Limited

"I really enjoy the challenge of educating each customer and the opportunity that each engagement offers to help facilitate a solution which takes them into a better, more secure place"

So, how long have you been involved in the IT disposal industry?

I'm relatively new to this industry having joined Greenworld just 2 years ago.

What was your background before this?

I was Chief Executive for a US software company working primarily in the aerospace and defence industry. Our software was used to capture and analyse failure data, covering the full product lifecycle; development through in-service to disposal. As you can imagine this information was incredibly sensitive to our clients; security was paramount. As Chief Executive, I was always mindful and responsible for the data protection of third party data; my signature was on more NDAs than you can imagine. It was here that I first experienced the issues with data sanitisation, both through life and end-of-life. I had to understand how we could assure our clients that at the end of each project, their data was securely sanitised.

What drew you into the industry?

Quite simply, I saw the job advertised and thought that it was a great opportunity to take my skills into a new area and into a company which I felt was ahead of the curve in understanding and resolving the issues of data on end-of-life equipment.

Have you seen many changes in the industry since you've been involved in it?

I feel the industry tends to move in cycles, as clients appear to shift their focus from risk aversion to cost cutting and then back again. One minute a company is almost complacent and happy to base their ITAD process on price and then suddenly, get themselves in a pickle as they attempt to batten down the hatches and lock up their children. This change in mind-set; from one to the other often appears to be influenced by the media covering the latest 'data loss' incident or fines imposed – suddenly the cost cutting exercises aren't so attractive.

What do you enjoy about the industry?

I really enjoy the challenge of educating each customer and the opportunity that each engagement offers to help facilitate a solution which takes them into a better, more secure place. There is a real sense of worth knowing that you are helping to protect their reputation and their client's identity!

What do you think are the main issues with the IT disposal industry at present?

Whilst there is an abundance of regulations and regulators which the end user has to comply with, there is a clear lack of guidance as to what they should do in order to be compliant. Furthermore, the industry itself is unregulated; leading to a huge variance in the services offered and delivered – some good and some not so… this leads to misguidance, misplaced confidence and massive exposure to risk.

What would you like to see improved within the industry?

I'd like to see clearer standardisation and guidelines developed for the end users and the introduction of standards governing those of us in the industry. This would help all parties have a clear set of guidelines for the ITAD activity. I would also like to see greater clarification and support of industry standards from central government; currently there is too much left open to interpretation.

What do you do to get away from work?

Other than spending time with my wife and two wonderful boys, I work on another passion, come obsession; a project I named 'Save our Towns' (www.saveourtowns.co.uk). This initiative aims to address the demise clearly visible in our towns and city centres across the UK. It is clear that our buying habits have changed over recent years. However unfortunately, the majority of retailers haven't changed to meet their customer's needs. Save our Towns aim is to bring together independent retailers, encouraging collaboration and helping them work towards common goals; creating initiatives that address their key problems. The retailers can't continue to wait for something to change; they have to make the change. I believe that in future generations we will lament the loss of our traditional high streets unless we act now!

To finish off, describe yourself in three words

Student, practitioner and facilitator – or to put it another way, 'Dad'.

Thank you for your time Simon and good luck with saving our towns!

Disclaimer: The comments here are those of the interviewee and do not represent the thoughts of ADISA and ADISA does not endorse the comments.

ADISA

INTRODUCING
THE ADISA ADTEST

The ADISA asset disposal test (adTEST) is the first security risk assessment of vulnerabilities during the IT asset disposal process. Assessing all participating elements, the adTEST allows data controllers to identify and address potential security and business risks which may exist within their asset disposal activities.
Don't wait for the news headline...KNOW YOUR RISK.

Incorporating a three stage methodology, adTEST is the most comprehensive review of asset disposal available today. Independently reviewing your current practices and procedures and those of your partners, adTEST identifies areas of concern and charts a path for remedial action.

In brief:

STAGE 1 - ASSESSMENT

A review of current policy to ensure that it is fit for purpose.

A review of contracts which are in place with any third party vendors to ensure work specification is detailed and clear for all.

STAGE 2 - OPERATIONS

A review of how your policy has been implemented by your departments and third parties.

Assessment of staff understanding of what is required of them.

Using GPS tracking devices ADISA monitors exactly where your assets go, who has access to them, and how long they take to reach their final destination.

STAGE 3 - FORENSIC

ADISA appointed forensic experts carry out an unannounced forensic audit on the processing facility where your assets are being handled.

Finished goods are seized and forensically analysed on site to see if any data is available and if that data is meaningful.

ADISA AD TEST DELIVERABLES

- Identification of contractual deficiencies in your downstream.
- Identification of all parties who handle your data carrying assets to ensure chain of custody is in place.
- Independent vigilance of your downstream partners.
- GAP Analysis of your policy verses your own current practice.
- Forensic Assurance that data has been destroyed.
- Full report for use in compliance with many regulatory requirements.

WWW.ADISA.ORG.UK

For further information please contact ADISA today on 0207 489 2008 or info@adisa.org.uk

Article 1 in the intelligent IT asset disposal series: "The need for data categorisation"

by John Sutton

Data categorisation (or classification) is the process of determining the business value (or sensitivity) of each piece of data that is owned by the organisation; data that is owned by other organisations (clients and suppliers), and personal information (relating to individuals).

Some data will be wholly unique to the organisation and the degree of protection afforded to such data is entirely the responsibility of the organisations. However, the protection of data that is not owned by the organisation will, in most cases, be subject to external controls such as legal compliance, contractual terms and conditions and government regulatory controls.

It is essential that the category of all data be determined before any information security control features, such as access and encryption controls, are deployed and utilised.

The same requirement also applies to the disposal or destruction of the data and its storage asset. Consequently, before any intelligent IT asset policy is written an organisation needs to ensure that a rigorous process of categorising the data is carried out.

Data categorisation requires that three different factors are considered and weighted:

Data confidentiality - some types of data may be freely distributed, while others must be kept more confidential. This factor is the most important in the categorisation process.

Data lifecycle - not all data needs to be retained for the same amount of time – some is of short term use only, while other data may need to be retained almost indefinitely. As data is categorised its lifespan must be identified.

Data value - While it is likely that the data's value is most closely linked with its sensitivity, this is not always the case. As such, it is good practice to establish the value of data to the enterprise independent of its sensitivity. A simple low, medium and high taxonomy is appropriate where a specific monetary value cannot be determined.

Unless all three factors are considered, the true business impact of a data compromise cannot be established. Without understanding business impact, decisions regarding data storage and protection cannot be made.

Data types

Data exists in two forms within an organisation:

Structured data - this is data that exists within enterprise databases.

Unstructured data - this exists in documents, e-mails, and other free-form sources. It is generally estimated that as much as 80% of an enterprise's data exists in an unstructured form.

Categorisation of structured data

Categorisation of structured data requires that each database as a whole be reviewed and the confidentiality, lifecycle and value be established. If data within the database have different levels of confidentiality, lifecycle and value, the most stringent applicable level must be applied to the whole database.

Categorisation of unstructured data

Categorisation of unstructured data is performed in much the same manner with the exception that a preceding step of data discovery is required.

Data discovery demands that every potential data source be reviewed to determine what type of data it contains so that appropriate categorisation can be applied.

This is a far longer and more laborious job simply because the data must be discovered before it can be categorised. This discovery process involves reviewing individual documents to determine their contents and then placing them in the appropriate cell in the matrix. This can be a very time-consuming process indeed.

There are data categorisation solutions that will search through an enterprises' storage systems, whether they are network, or even work-station based. These solutions will grab standard document metadata (file-type, name, owner, creation date, last access date, etc.) as well as specified content data.

By scanning through documents for keywords and patterns (e.g. those associated with credit card numbers), these solutions can build a structured list of documents for review. Discovered documents do need to be manually reviewed to determine the actual business impact so that the actual categorisation can be applied. However, the automatic discovery and structuring of the lists expedites the categorisation process as a whole.

Data categorisation matrix

Once the categorisation of all data types has been completed, it is then useful for the outcomes to be presented in an easily readable form such as a data categorisation matrix.

Business impact level tables

The final step in the data categorisation process is to present the information in the form of a business impact level (BIL), and create a separate table for each of the data owners.

Individual organisations should decide on how many BILs best suit their business needs. SMEs may find a straight-forward three-level model of LOW, MEDIUM and HIGH meets their needs, whereas a large national or international business would use a five-level model. The UK government uses a seven-level model.

The BIL table provides a framework that allows organisations to assess the BIL for compromises of the confidentiality of information and ICT systems.

(NB: BIL tables are also used to assess the compromises of data integrity and availability. It is usual to only consider compromises of data confidentiality for asset disposal purposes).

The development of BILs will feature in the next issue.

Industry news

Record fine from the Information Commissioner's Office.

Whilst still under appeal, the ICO has shown its appetite to fine those companies with improper disposal activities with a proposed record £375,000 fine on Brighton and Sussex Hospital. Specific details are yet to be confirmed, but it is understood via general press that a service provider who was meant to perform onsite data sanitisation failed in the task with around 20% of drives being unaccounted for – some of which were identified on e-bay.

Tabernus open UK office

A recent addition to CESG approved software list; Tabernus, a US headquartered company, has opened a UK office with Daniel Dyer fronting all UK operations. **www.tabernusuk.co.uk**

New European Sales Director at Blancco

News from Blancco is that Daniel Smith (formerly UK Country Manager) has from January 1st accepted the new role of European Sales Director, which now sees him attempting to replicate the success of the UK in other areas. **www.blancco.co.uk**

News from Kroll Ontrack

Charmayne Simmonds has stepped into the shoes vacated by Donal Thorburn to drive the UK Data Erasure business at Kroll Ontrack. Responsible for new business development across the suite of Data Management Software and Tape Solutions, Charmayne took on the role in November and is looking forward to driving new business opportunities for Kroll Ontrack – particularly within the ITADs. **www.krollontrack.co.uk**

Stronger and fitter: the new BTR

BTR UK, Britain's Trusted Recycler has new owners and has just completed and moved into brand new state-of-the-art premises. The business recently went through a financial restructure and ITAS Global and four key members of the original management team joined forces to purchase the business, trademarks and branding of BTR UK in January 2012. Security of jobs was important to the team, so they are proud that 70% of positions were protected. Clients as diverse as government authorities to charities and NHS to private organisations are delighted with the consistent and trusted approach taken by the business. "Continuity of operations has been smooth" commented Chris Taylor, Re-marketing and Ops Director. John Atkins, Business Development Director told ADISA he is ecstatic that "within two months of trading we have won further new business from our partners and assured them in achieving fresh and USP-inspired wins against competitors". As well as moving around the corner from Birchwood Park, Warrington in a short period of time, downtime was almost non-existent whilst maintaining customer service level targets. A silver-accredited Blancco partner, BTR goes from strength to strength. **www.btruk.com**

LOOP uses recycled IT to help Malawi orphanage

Last November Loop Computer Reuse visited Mchinji in Malawi, Africa. Despite the poverty of the country and lack of new equipment, the people of Malawi have the tenacity to keep using and extending the life of equipment, which in the UK would have been sent to a recycling plant.

In Mchinji, they were able to guide the resident technicians at a school for orphaned children on how to reuse their computer equipment. By the end of the trip they had 24 machines working for over 200 children to use. This was achieved despite power cuts and bad weather.

The moral of this story is that there is an alternative to recycling, and if you do have any computer equipment that could be put to a better use, then Loop knows a group of Malawians that would be very pleased to hear from you.

RDC open new European headquarters

In January 2012, RDC moved to operate from a 350,000 square foot head office and operational facility in Braintree, Essex. The move creates one of the largest IT asset recovery and deployment service sites in Europe, and facilitates the continued expansion plans for RDC ITAD services in the UK and overseas. **www.rdc.co.uk**

Sims Recycling Solutions acquire mobile phone refurbisher

Sims has expanded its asset recovery business into mobile devices, with the acquisition (for an undisclosed fee) of S3 Interactive Limited (S3i). Glasgow-based S3i is a specialist company for the recovery, repair and refurbishment of devices such as smart phones and tablet computers, and this purchase further enhances the service specialism within Sims Lifecycle Services portfolio. **www.uk.simsrecycling.com**

EOL appoint new Managing Director

Wendy Davies was confirmed on January 1st as the new Managing Director at EOL Lifecycle Services Limited. Wendy comes from a supply chain background with previous roles at Airbus, Rolls Royce and BAE. Davies explains, "My vision at EOL is to help improve the current perception of IT asset disposal companies by raising the bar of service delivery and customer service. We want to help our customers understand risk within their disposal programs, and help them manage that risk to a minimal level whilst maximising reuse and residual return. My commitment throughout this process is first to security, then to value and, of course, helping fight the illegal exporting of WEEE". **www.eolitservices.co.uk**

To announce news about your business in the September edition please email submissions@adisa.org.uk.

ITAD classifieds

Byteback IT Solutions Ltd
Unit 5, The Gatehouse Centre, Bristol, BS13 9JN
Tel: 0117 3706 456 www.byteback.org.uk

USING YOUR UNWANTED IT EQUIPMENT TO BENEFIT YOUR COMMUNITY

Services - computer/WEEE disposal, reuse, and recycling. Data destruction services.

Reusing equipment locally. Secure data destruction using CESG approved data erasure software and physical destruction methods.

Computer Aid International
10 Bruswick Industrial Park, Brunswick Way, London, N11 1JL
Tel: 020 8361 5540 www.computeraid.org/donate

Donate your computers to charity!

Computer Aid International offers a complete service to companies replacing their IT hardware. We are experts in end-of life IT asset management, including data destruction, computer refurbishment, reuse, and recycling.

For more information about our services please email enquiries@computeraid.org.

Concept Management
Royal House, Tennyson Street, Bolton, Lancs BL1 3HW
Tel: 01204 396662 www.conceptmanagementuk.com

Concept provides a compliant service encapsulating Environment Agency Approvals and European WEEE Directives.

We provide a FREE OF CHARGE documented, totally secure collection as a Certified ADISA Member.

We provide onsite and offsite destruction using CESG approved crusher and degausser, shredder and drives wiped to BS Infosec Enhanced Standard 5.

Disk-Demolition.co.uk
Unit 32, Anniesland Business Park, Glasgow, G13 1EU
Tel: 0845 519 7626 www.Disk-Demolition.co.uk

Specialist IT asset disposal: ISO 9001 and ISO 27001 certified computer/WEEE disposal, reuse, recycling and onsite data destruction services.

Promoting equipment reuse, ensuring data confidentiality with Government CESG approved data erasure software and physical destruction equipment.

EOL IT Services
1 – 3 Baltic Wharf, Station Road, Maldon, Essex, CM9 4LQ
Tel: 0845 600 4696 www.eolitservices.co.uk

Professional IT asset disposal and data security company: ADISA, ISO 9001 and ISO 27001 certified computer/WEEE disposal, recycling, onsite and offsite data destruction services.

IT delivery or relocation throughout the UK and Europe, IT equipment cleaned and sanitised, supply of spare IT parts/components also provided.

eReco EMEA Corp Ltd
17&34 Hobbs Industrial Estate, Newchapel, Surrey RH7 6HN
Tel: 01342 833033 www.ereco.co.uk Jane Taylor janet@ereco.co.uk

eReco specialises in providing professional, efficient and flexible IT and electrical disposal and remarketing services. We offer service nationally using our own staff and vehicles so you'll find us secure and cost effective. ISO 9001, ISO14001 and working with ADISA towards certification.

Flection Group
Unit 49 Hirwaun Ind Est, Aberdare, CF44 9UP
Tel: 01685 819210 www.flection.com

"EU WIDE ICT ASSET RECOVERY, DISPOSAL AND RECYCLING" Eco-friendly processing, covering all compliances for WEEE and data security of IT equipment whilst obtaining maximum return for your computer equipment.

Hamilton Asset Management
Unit 6 The Heathrow Estate, Silver Jubilee Way, Hounslow, TW4 6NF Tel: 01344401342 www.hamilton-am.co.uk

Specialist IT asset disposal ISO accredited, ADISA certified computer/WEEE disposal, re-marketing, redeployment, recycling and onsite data destruction services

Promoting the reuse and remarketing of assets, ensuring data security with CESG approved methods and physical destruction

ITAS Global
t/a BTR UK Unit 7, Westway 21, Chesford Grange, Warrington, WA1 4SZ
Tel: 01925 846660 www.btruk.com

Specialist IT Services: Specialist channel partner working with many of the UK's leading service providers, manufacturers, government organisations and some of the Top 5 banks in the UK, ISO 9001 certified computer/WEEE disposal, remarketing, recycling, onsite data destruction & installation services ensuring data confidentiality as a Blancco preferred silver partner.

Loop Computer Reuse C.I.C
East Malling Enterprise Centre, New Road, East Malling, Kent, ME19 6BJ
Tel: 01732 522230 www.loop-cr.co.uk

Loop Computer Reuse is a community interest company specialising in the reuse of IT assets. For a total solution to your redundant IT contact Loop Computer Reuse.

Oden Services UK Ltd
Unit 23, The Tanneries, Havant, Hampshire, PO9 1JB
Tel: 02392 477991 www.odenservicesuk.co.uk

ISO9001 IT service parts supply chain solutions and Recycling IT WEEE Asset Disposal conforming to ISO14001. We can provide onsite or offsite services using government CESG approved software.

Contact info@odenservicesuk.co.uk

Reuse Recycle IT
Unit 3J, Barlow Way, Fairview Industrial Park, Rainham, RM13 8BT
Tel: 0844 7702380 www.reuserecycleit.co.uk

Reuse Recycle IT is a specialist secure IT disposal and remarketing company, offering low cost, seamless and transparent IT disposal solutions using our comprehensive driven systems to track your assets and maximise your revenue.

SWEEEP
Gas Road, Sittingbourne, Kent, ME10 2QB
Tel: 01795 434125 www.sweeep.co.uk

Launched in 2006, Sweeep quickly made an impact on the WEEE recycling marketplace. The recent partnering with Kuusakoski Oy has further strengthened their offering allowing for investment in high security per-treatment, enhanced QZ in-feeds, re-developed CRT processing and a revolutionary furnace to produce lead from CRT glass.

Next issue - September 2012

Publication theme: The Waste and Crime edition

Feature article 1:

With the EU WEEE recast due to be in place are there any differences to the B2B requirements which we should know about?

A leading expert on the WEEE re-cast from government will explain what the changes actually mean.

Feature article 2:

Taking source material from Jason Warner of Harvard University and award winning Ghanaian journalist George Sydney Abugri, this feature exposes criminal activity taking place as a result of data found in e-waste in Africa.

Feature article 3:

Adrian Price, Office of the CIO – Ministry of Defence, explains why control over asset disposal is essential for any security conscious organisation.

The results of the ADISA 2012 survey will also be published. This survey is taking place in May and will focus on the trends and issues in the UK ITAD marketplace.

Regular features such as:

- The continuation of the "Intelligent IT disposal" article
- An interview with a leading participant within the IT disposal marketplace
- Industry news and updates.

Image courtesy of Greenpeace

Subscription:

This is a free of charge subscription magazine.

To ensure you receive your copy please email: magazine@adisa.org.uk with your name, title and postal address.

Copies of all articles can be downloaded in full from the ADISA affiliate members website.

Article submission:

To submit news about your business or an article on the industry, please send copy to submissions@adisa.org.uk

For any other enquiry please go through the press office on press@adisa.org.uk

What do you need to erase today?

blancco

CERTIFIED DATA ERASURE

Erasure solutions for your every need

Everyday, tens of thousands of IT assets are sanitized, analyzed and tested using Blancco solutions. As the global leader in data erasure and computer reuse solutions, Blancco is the preferred erasure choice of commercial, public sector, and trade organizations.

- 100% secure erasure.
- Fastest erasure process.
- Most certified data erasure software in the world.

Contact the Blancco UK Team
Call: +44 1279 874 200
Email: uksales@blancco.com
www.blancco.co.uk