ADISA

WINTER 2014 ISSUE 4

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

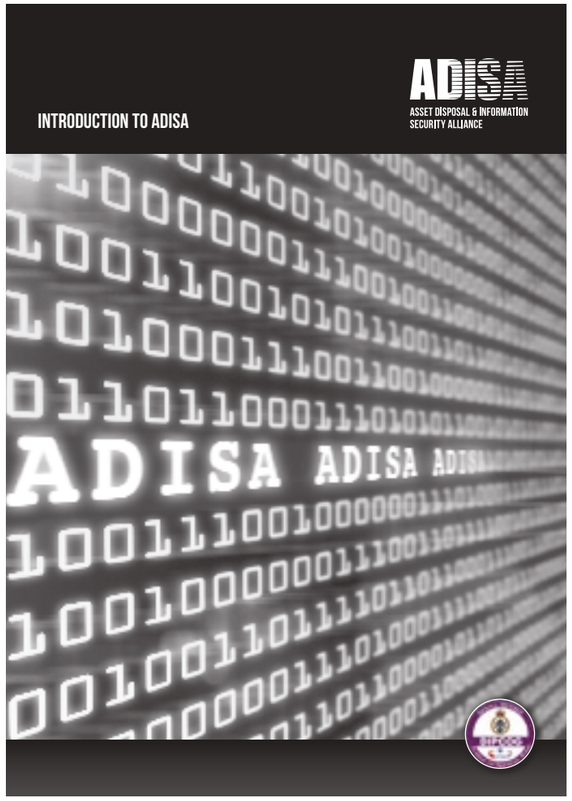
THE ADISA MAGAZINE IS BACK!
THROWING THE SPOTLIGHT ON IT ASSET DISPOSAL

FEATURE
ERASING THE DATA ON SOLID STATE DRIVES
PAGE 4

FEATURE
THE CHANGING FACE OF DATA PROTECTION
PAGE 17

FIND OUT MORE ABOUT ADISA BY DOWNLOADING ONE OF OUR BROCHURES:

FOR INDUSTRY:



FOR END USER:

ADISA

ADISA.ORG.UK

EDITORIAL WINTER 2014

Well we're back!!! It's over 12 months since our third magazine was published in September 2013 and this 12 month hiatus is entirely self-imposed. Due to escalating print costs a decision was made after edition three to revert to an e-zine (which you are now receiving) but with the lack of a print deadline and ever increasing business pressures I'm sorry to say that the magazine slipped further down the to-do list... until now!

The ADISA magazine is back and will be published in two editions, winter and summer. You will note that the level of advertising is significantly reduced. This is as a result of the significant decrease in cost for publication and therefore we felt it more appropriate to try to create a less commercial feel for the magazine and make it as informative as possible.

As this is our first magazine for some time we do not have a theme as such but we will cover a wide range of topics relevant to the industry so that we can re-introduce the corporate reader to the subject matter and some of the challenges faced.

Our feature article is on a familiar theme – solid state devices. In issue 1, Gerry Masters went through the technical aspects of solid state overwriting and now, nearly two years on, there is still little understanding of what the industry and its customers, should do to promote the re-use of these devices. Professor Andrew Blyth and myself, have been working on SSD since summer 2012 and Andrew has tested overwriting solutions for several leading software vendors. This article details his findings and makes recommendations for how corporate end users can manage risk associated with this technology at end of life.

Our second article combines many of the presentations myself and Alastair Barter of the ICO (See issue 2) have given in terms of an update of the proposed changes to the EU Data Protection Directive. The aim of this article is to pull together many of the rumours and to highlight critical changes which are coming in 2015.

We also have an excellent piece from the CEO of ASVIDA® in Asia. This focuses on how changes in IT infrastructure are driving growth and creating opportunity.

We're delighted to welcome guest writers, Nigel Jones–Morris from NHS Surrey and Borders, Alex MacColl from MacColl Media, and Kow Ya from ADVIDA® in Asia.

EDITORS
Steve Mellings

COPY EDITOR
Paul Dalling

CONTENT AUTHORS
Steve Mellings
Professor Andrew Blyth
Nigel Jones- Morris
Alex MacColl
Kow Ya

DESIGN
Antoney Calvert at Colourform Creative Studio

PRODUCTION
Antoney Calvert

ADVERTISING ENQUIRIES
magazine@adisa.org.uk

CONTENT ENQUIRIES
Steve Mellings
steve.mellings@adisa.org.uk

ADISA
Hamilton House,
1 Temple Avenue,
London, EC4Y 0HA

Tel: +44 (0) 845 557 7726

CONTENTS

STEVE MELLINGS, ADISA, PROFESSOR ANDREW BLYTH, UNIVERSITY OF SOUTH WALES.

ERASING THE DATA ON SOLID STATE DRIVES

How and where we work has changed dramatically in the past 10 years. Users now demand the ability to work where they like, which has seen technology move from desk based devices to a multitude of different platforms used in the work place. Manufacturers have re-energised the market by introducing smaller, lighter, but more powerful devices, which has allowed more productive working practices to evolve. Consequently working on trains, in hotels and at home have now all become part and parcel of everyday life.

A key component in facilitating this has been the evolution of NAND based storage technology. Commonly referred to as Solid State Drives (SSD), this new small form factor storage has allowed devices to become more portable, faster and more utilitarian. Adoption of this technology has led to a series of challenges later within the product lifecycle, which were perhaps not considered at the point of deployment.

Issues surrounding device security and management are well documented but new concerns have emerged regarding the retirement of these assets. Too many businesses are unaware of the challenge of competently erasing SSD and are either allowing uncontrolled risk into the organisation or are adopting a risk avoidance approach at end of life.

So what are these issues and how can we resolve them?

This article gives a high level overview of the issues of SSD overwriting and offers some advice on how to overcome them.

WHAT ARE SOLID STATE DRIVES AND WHAT ARE THE CHALLENGES OF DATA OVERWRITING?

SSD are storage devices, which utilise NAND cells for storage and controller chips for device management and user interface. (See Figure 1) A key part of SSD architecture is over provisioning. This is where the total storage within each device is greater than the available storage to the user and is intended to extend the life of the device.

There are a range of technical functions that happen during the operation of SSD including wear levelling, garbage collection and data compression. During in-life use, these process are the very core of the benefit of using SSD but at end of life they become a significant handicap when validating traditional data overwriting techniques.

Traditional overwriting (commonly referred to as data erasure) is achieved by writing a series of characters to all addressable areas of a magnetic hard drive. Validating that this has occurred is easy, as a sample of sectors can be read to confirm that either (a) there is no information present or (b) that consistent overwriting patterns are in place.

FOR SSD OVERWRITING THERE ARE DIFFERENT APPROACHES, THREE OF THE MOST COMMON ARE:

1. A known pattern of data is written from the start of the device to the end of the device. The number of times that this process is repeated is derived from the implementation of the wear levelling algorithm. The algorithm is implemented differently by each vendor and on different devices from the same vendor, so the number of necessary overwrites to successfully remove all data varies.
2. A SSD USB controller chip implements a secure erasure command, which will then either make use of a software solution or a hardware solution to erase all of the data on the NAND storage cells.
3. A form of crypto erase is possible whereby the encryption key is located and erased. This is an extremely challenging approach as for obvious reasons the location of these keys is not widely known!

The key problem when dealing with SSD is how do we validate that the overwriting process has been successful? A successful overwrite could be measured in two ways; (a) that all physical memory locations have been included in the overwrite and (b) that there is no data recoverable using forensic techniques.

Confirming a successful overwrite is an issue, as there is no one to one mapping of data locations due to over provisioning. Furthermore when a cell fails or reaches its maximum read/write it becomes degraded and not addressable. This effectively leaves data still resident on such cells after an overwrite has been instigated through the controller chip.

For this reason existing approval schemes, such as CAPS run by CESG, cannot validate an overwriting software as arguably there could be degraded cells on a device and as such data may remain.

A further issue is that SSD is a new technology and the manufacturers' of these devices do not follow consistent protocols during manufacturer. Chip substitution is commonplace, which means that the same brand of SSD may have different manufactures' components inside. As the controller chip functions are potentially implemented differently depending on manufacturer then the question of "what SSD do I have?" must become one of "what chips sets are within my SSD estate?"

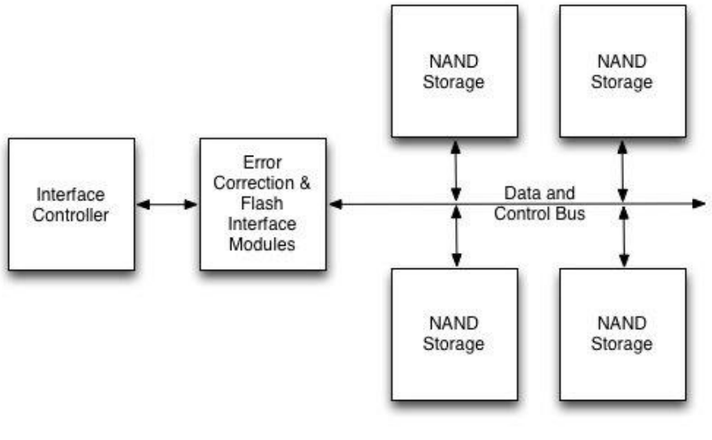


Figure 1 – SSD Conceptual Architecture

THE SOLUTION WHEN DEALING WITH END OF LIFE SSD?

Confused? At this stage most companies when they are aware of these issues will say, "Destroy". It's the easiest process to implement and allows companies to manage their risk. However, to simply destroy assets, which in some cases, will hold up to 25% of the original value, is wasteful, not only in an environmental sense but also financially.. So what to do?

Unlike overwriting for magnetic hard drives, there is no single absolute statement, which can be relied on to make you, the risk owner, feel comfortable. As such each risk owner must make an informed, risk based decision on how to deal with SSD at end of life. This may sound daunting but the good news is that by following the steps below, we believe that by adopting a risk base approved to SSD overwriting, that you will be able to understand the risk and build in the correct procedural and technical countermeasures.

THERE ARE 5 KEY STAGES TO SECURE ASSET DISPOSAL AND THESE SHOULD BE FOLLOWED REGARDLESS OF THE MEDIA TYPE. THESE ARE:

STAGE 1: POLICY DEVELOPMENT

- Display management control through a prescriptive asset disposal policy. This should include data categorization, business impact, threat profiling, risk assessment and finally, this should produce an approved media sanitisation profile. (See Appendix B.)

STAGE 2: ORGANISATIONAL CONTROL

- Process and Procedure documents are required to help deliver policy. For this reason, any media that is being disposed of should be done so in a controlled way. A phrase used by regulators both in the UK and the US is "organisational control". Clearly if there is no control over the process, then can any company confidently state that they can show "organisational control?"

STAGE 3: THIRD PARTY CONTROL

- Control all external engagements with a clearly defined service specification as part of a written contract. This should include ALL potential outputs from the business, including end of life, end of lease and mid-life instances such as repair. Look for relevant standards, which show independent assessment of their security capabilities. [11]

STAGE 4: COMPLIANCE

- To be able to show compliance with your own policy (which in turn should show corporate compliance to regulatory requirements), a thorough audit programme is required which should result in a reporting schedule able to evidence control over this process.

STAGE 5: REVIEW AND REFLECTION

- Technology changes, partners change and threats change, so it is essential to review and consider approaches to asset disposal at regular intervals.

> **As we are talking specifically about SSD** let us drill down into Stage 1 in greater detail and in particular how to decide on an approved means of sanitisation for SSD.

STEP 1 TO BUILDING AN APPROVED MEANS OF SANITISATION FOR SSD

DATA CATEGORISATION:

- It is essential to consider the category of data, which your company controls. At a superficial level, if it is data that sits entirely in the public domain, then the category would be very low (it is publicly available anyway). However, most businesses hold data pertaining to an individual (pay roll for example) or their own corporate data, which ensures that their data should be handled in a protective manner. How data is categorised is entirely up to the company and there will be different approaches to data protection depending on the data category. Perhaps a three-phased approach of public, official or secret could be used?

BUSINESS IMPACT:

- Once categorized, the impact to the business of the breach of that data should also be assessed. Whilst the payroll of the CEO would be categorized as highly sensitive, its breach would only cause minor impact to the business (perhaps with some shareholder dissonance!) whereas the loss of the entire staff payroll would cause significant impact to the business. Almost certainly resulting in regulatory action, the fines associated with such a breach would be significant, but also the cost of addressing the breach would be equally significant.

THREAT PROFILING:

- Who potentially could be targeting you? Thanks to the proliferation of the dark net, hacking skills (SKS Cyber skills) are now being shared, meaning that the volume of bedroom hackers has grown exponentially, which has largely been the cause in the proliferation of cyber-attacks being carried out. Organised crime has also been quick to skill up in technology and are ever more resourceful when looking to seek new ways of sourcing funds. So who potentially is targeting you? What is their motivation? What are their skills?

STEP 2: IDENTIFICATION OF SSD ASSETS

It is essential to identify where SSD sit within your business, such that all possible outputs are aligned to the same policy. Product sets such as laptops, tablets and smart phones need to be included as well as potential hidden SSD within networking equipment or even printer technology. Regardless of the media being discussed, the creation and management of the chain of custody IS ESSENTIAL and without this being in place not only is asset leakage inevitable but regulatory compliance impossible to prove.

STEP 3: RISK ASSESSMENT

Once we have gone through these stages then a risk assessment can be made. This assessment should look at the processes surrounding asset retirement, as well as the endpoint sanitisation technique required. As we are focussed just on the act of sanitisation we should re-introduce your options.

Physical Destruction; some traditional hard drive destruction techniques won't work on SSD simply because of the physical nature of the product. Some larger shred sizes may damage the boards but could miss the NAND cells themselves resulting in potential cell level recovery. SSD destruction should be achieved in such a way where every NAND cell is impacted and for higher levels of attack, the potential requirement for them to be disintegrated may come into play.

Degaussing; theoretically if a magnetic waveform was so strong and used on a SSD it could erase SSD, as it could force all the electrons within the NAND cells to revert to a single state. However, current commercial degaussers do not work at this high level (and it is unlikely they ever will) and therefore won't work on SSD.

Overwriting; in 2013 we published a methodology for testing over-writing solutions used on SSD [10]. During this we discovered that based on various degrees of forensic attacks, data cannot be recovered from a particular set of SSD after being overwritten. It is worthwhile reviewing this methodology and looking at some of the results, which have been found on commercially available products. Sadly we have been unable to offer confidence that "Product X works on all SSD", because we have found SSDs (particularly earlier SSDs) to be manufactured differently and also that our assurance of the inability to perform data recovery is based not on conclusive evidence of an overwriting pattern, but that at a cell level hardware encryption was being invoked, which meant that even after intrusive and destructive attacks, all that could be seen was encrypted data. (Whether than is the original data pattern or overwrite is impossible to gauge.)

STEP 4: DECISION ON THE APPROVED MEANS OF SANITISATION

At this stage there should be an understanding of the category of the data, the impact of that data loss and where the threat may be coming from. A risk assessment can now be made for deciding on the appropriate means of sanitisation. For those seeking to promote the re-use of assets we would always recommend that any decision should include the use of products which have been forensically tested. This forensic testing can follow a similar method which ADISA advocates, or can follow a method which the risk owner themselves approves. However, due to the nature of the technology it is essential that testing is carried out. For legal compliance it is also recommended to seek products which offer the additional benefit of an audit trail (serial number reporting) and indemnity insurance.

An example of an approved means of sanitisation is shown in Appendix B and it is crucial to look at the processes included BEFORE sanitisation. Like all security, the biggest vulnerability lies not in the technology, but in the people around it, so don't forget that inventory management (chain of custody), partner management and verification of the service being executed is perhaps the most important part of all. After all, if a device doesn't make it to the bench to be sanitized, then all of the above is academic!

SUMMARY

Most organisations when asked are not aware of the issues of end of life SSD processing and so the issue only becomes critical at the time when the process is required. This short timeline results in risk avoidance rather than risk management and so the key to SSD at end of life is to engage in the process BEFORE you need it!

Data controllers should engage with recognised software developers, engage with their IT asset disposal (ITAD partners) and engage with forensic experts. Together, you CAN control risk and ensure that you meet the requirements of the data/privacy regulators, your own data protection requirements, whilst at the same time promoting re-use and benefiting from the residual value locked within these assets.

Whilst content of this paper is applicable to any flash based storage device, the conclusions should only be considered with reference to devices that are utilising the SSD controller chips to access Flash/NAND storage cells. For products such as smart phones we would reference research undertake by the author, which will be released in March 2015. For devices such as USB sticks, digital cameras and smart phones that do not utilise SSD controller chips to access NAND storage cells, many of the research findings in this paper will not be applicable.

NIGEL JONES-MORRIS

IMPROVING RISK MANAGEMENT WITHIN THE NHS ASSET DISPOSAL PROCESS

I was mildly surprised when my manager offered me the opportunity to attend a course on IT Asset Disposal (ITAD), run by ADISA. Although it turned out to be excellent value for money, it still represented a sizeable investment for an NHS Trust in these austere times.

Besides, I'd been disposing of redundant IT equipment for over 10 years with no hiccups. This dated back to a time when the directive was "do it, do it well, and do it for free".

So what does doing it well entail in the ITAD world? Keeping your data secure? Minimising impact on the environment? Maximising return on investment by reselling working components? Recycling parts that cannot be re-used?

Of course, these days the answer is "all of the above", though I can't be sure if that was one of the questions in the University of Glamorgan run examination at the end of the course. A 30 minute, 30 question multiple choice paper followed by a two hour handwritten paper. Two hours! That's about 119 minutes longer than I had previously handwritten for in… well, a very long time!

The exam was certainly very thorough, but then so had the preceding two days been. I felt prepared not only for the exam, but for the real world awaiting me on my return to work.

By the end of day one, my preoccupying thought was, in hindsight, how lucky I had been in doing what I had been doing for so long, without ever being caught! I.e. incurring the wrath of the Information Commissioner's Office (ICO).

Sure I had chosen my ITAD suppliers with a degree of care, but for a long time the key part of my directive was getting redundant IT equipment disposed of for free. Ten years ago the environment wasn't at the forefront of our minds as it is today, and to be completely honest, nor was data security. Getting a return on reusable and recyclable parts? That hadn't been considered at all. Allowing our supplier to sell on what they could, to recoup their expenses in making the collection and arranging proper disposal was as good as it got, and I paid little attention to where our assets would end up.

I am no fool, and am fully aware there is no such thing as "something for nothing". I realise that my previous ITAD suppliers were going to do something to cover their costs, and indeed make a profit. Just because I work in the public sector it doesn't mean I think profit is a dirty word. It's a perfectly reasonable, expected even, part of being in business and I certainly hope that no company I have previously dealt with ever bore any losses as a result.

I did not, however, pay any attention to the details of how their costs were recovered. Other NHS Trusts have since learnt to their cost, that overlooking this can be a very expensive business. Hard disks containing personal identifiable data found their way onto the open market via a well-known online market place, and suddenly the Directors of all NHS Trusts have 200,000 reasons why IT Asset Disposal needs to be carried out using a thorough, efficient, secure, and cost effective process.

Luckily I had previously selected reputable companies, and none of our data assets fell into the wrong hands. I am under no illusions though, this was as they say, "more luck than judgement".

The ADISA Certified Professional Course thoroughly prepares you, and enables you to take any element of luck out of the equation. The first course had room for improvement, and I believe future candidates will benefit from that. For me, I don't think enough time was spent on covering the contract tendering process, although they included questions on that in the exam. Again, from a purely personal perspective perhaps too much time was spent covering how to protect data from foreign intelligence agencies, which perhaps naively I don't think will ever be too much of a concern for me. Having said that it is important to note the course is not aimed purely at the NHS. Amongst my fellow students there were also representatives from large private sector companies, and people working for foreign governments – who I'm sure would have found these topics useful

Some people's main concern was data security, for others cost remained high on the agenda, and for some the impact on the environment, recycling and passing equipment on to charitable organisations were the reasons they attended the course.

Data confidentiality was the core of one exercise. It was drummed into us never to refer to redundant IT equipment as waste. The term 'waste' can indicate a low level of importance and lead to the job not being given the attention it deserves, and on to mistakes being made. Your data, contained on any one of a number of devices to be considered, is certainly not waste, it's an asset. ITAD is not waste management, it's a part of the asset management process.

The key message for me was risk. Balancing risk against cost in order to get the job done effectively, taking into account sanitisation methods, departmental security policy, asset disposal policy, supplier selection, cost, brand protection, environmental protection, software licensing, UK Law and of course verifying compliance.

I also benefited from a great networking opportunity in the form of a night out with my fellow candidates, superbly hosted by Steve Mellings, co-founder of ADISA. This gave us the chance to compare notes, discuss the course and start planning how we would put our new found knowledge into use at the earliest opportunity. The food and drink wasn't bad either.

Nigel Jones-Morris

ALEX MACCOLL, MACCOLL MEDIA

IOS8 QUAGMIRE

The September launch of iOS8, much like iOS7 the previous year brought with it much fanfare and press attention, not to mention new devices (iPhone 6/6Plus and iPad Air 2) and has generated some of the strongest sales for Apple mobile devices since launch. The troubling issue of iCloud Activation Lock continues to slow processes and potentially reduce value, and it's becoming somewhat of a quagmire for the ITAD industry.

On paper, it's a simple and very useful feature for most end users. A pre-selected setting called "Find My iPhone" automatically enables "Activation Lock", which ties the device (iPhone, iPod or iPad running iOS7 or iOS8 – currently all devices bar iPhone 1/3G and iPad 1st Gen) to a specific Apple ID. The idea is that before the device can be erased and reactivated, it must be unlocked and the features disabled by the user. It's an effective security feature, especially as these devices are so attractive to thieves – and it's an especially useful feature for company fleets, which may have sensitive data stored on them.

The major drawback of this feature is that unless the end user individually resets the devices and disables Find My iPhone and Activation Lock, by the time the device passes onto an ITAD it is unsalable as it will not activate with Apple's servers. Whilst data can now be erased securely, the Apple ID remains visible and the correct password must be inputted before the device can be re-used.

And it's not for lack of trying to find an alternative solution – there is no usable method available to remove the activation lock without validation, furthermore any method would be on the wrong side of the law.

Speaking about the problem, Steve Inglessis of Blancco UK said, "It's still a work in progress. Apple aren't going to be giving us or anyone else the required access or an API for their database so that we can cross check and release the device from the registered email address. In this sense it's very much like the age-old issue presented with Blackberry and their PIN system. Whist Blancco erases the device itself, we can't legally or otherwise release the registered details, as the device is identified by IMEI when re-registering with iTunes."

The whole situation is, I suspect, a veiled attempt by Apple to slow down the used market with regards to iOS devices, albeit bringing with it a genuinely good security feature for users of iOS devices. Resale values of iOS products remain strong, but this problem will hit the ITAD industry, so it's important that end users are well informed that these kind of devices must have Activation Lock turned off, in order to realise their true value.

The best method to do this is on an individual basis, and is as follows: go to Settings > General > Reset. Once the user erases the content, Find my iPhone and Activation Lock are automatically switched off, and the phone can be erased securely and re-activated.

Demand for iOS devices is consistently on the up, and this is just another hurdle that ITADs have to jump over in order to take a share of that revenue.

SPOTLIGHT ON...

JAN SMITH – FOUNDER AND CEO OF EOL IT SERVICES LIMITED

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

EOL started in 1996 so we're heading towards 20 years.

What was your background before this?

Prior to EOL I had been involved in the IT industry for 25 years, mainly within the channel but always customer facing.

What drew you into the industry?

I was looking for the next growth area, which I saw as IT security and disposal back in 1996. It was still very embryonic, but it was clear here was a huge opportunity within the product lifecycle. In the beginning, we focussed mainly on the desktop area. Our customer facing skills were quickly utilised and implemented taking on other areas and a wider range of services, developing from a very early stage.

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

The sector has matured since we started now offering a more professional approach than before. We have also seen in recent years a significant divide between companies building a long term future in this sector versus those that would be described as "fly-by-nights". The former are those companies offering well priced quality services with the other end of the market, focussed on price alone. This model is evolving and it is clear that as customers become more aware they have begun to see the difference between the two ends of the sector.

What do you enjoy about the industry?

Personally I enjoy this sector as it continues to evolve and improve at quite a pace. It is challenging that after nearly 20 years' experience, we continue to work hard to remain at the forefront of this industry. The momentum and pace is as strong as we have ever seen. A mood change within the industry to raise standards continues. Being part of this movement is exciting and helping customers see the sector differently is both challenging and innovative.

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

There is a huge amount of naivety particularly within the public sector over data security. Customers, private or public, have two options: one- a secure chain of custody - or two, an insecure chain of custody. There is far too much focus on price rather than quality or security. Public service tenders we see released are out of touch with commercial demands. The private commercial sector are motivated and challenged to learn and adopt the policies and strategies that we promote. After all, we carry out this work day-in-day-out and should be classed as the experts who can be relied upon. If we as a sector, do not get this right, there is nowhere for us to go. It is obvious that once an organisation trusts your ethics in the UK they want to replicate this in other territories. EOL's expansion of services into Europe has been both exciting and challenging.

What would you like to see improved within the industry?

I'd like to see the industry pull together and present itself to the customer in a more professional way. The ADISA platform has been a good starting point but too many organisations still sell on price alone versus those of us who always promote a quality secure service. Our clients have to understand that asset disposal is an important part of the business process which has data security as its number one priority. Too much focus is made on the act of data erasure with cold comfort given by meaningless certificates. Proof of a quality service is often ignored or seeks little demand. Many customers fail to grasp that a proper understanding of the chain of custody is essential to manage the processes surrounding sanitisation and data security. End users need to see this process as much more than redundant IT equipment. It's an afterthought for many and deemed easy to administer. I can assure you it is not. The processes developed, implemented and adhered to since our inception in 1996 continues to ask searching and challenging questions. The diverse range of equipment we handle forms many sorts of legacy systems, developing a vast skill set for our engineers, possibly the most highly trained, on multiple platforms, in the field.

What changes do you think will happen within the industry within the next 3 – 5 years?

We are already seeing more clients taking the correct level of interest in our sector. With greater auditing and questioning of proof of security occurring. I hope that ADISA will become more widely recognised as that will help end users identify the correct authority in this marketplace. Shorter term, we are seeing an increase from our customers in their requirement for hard drive shredding, but an even greater increase in quality and diverse services.

What do you do to get away from work?

Relax, walk and write. I'm currently working on an idea for a series of children's books. I'm also a budding inventor, the most recent of which EOL will take to market in 2015. I love to spend time with people I enjoy the company of, which thankfully is also my family.

To finish off, describe yourself in 3 words.

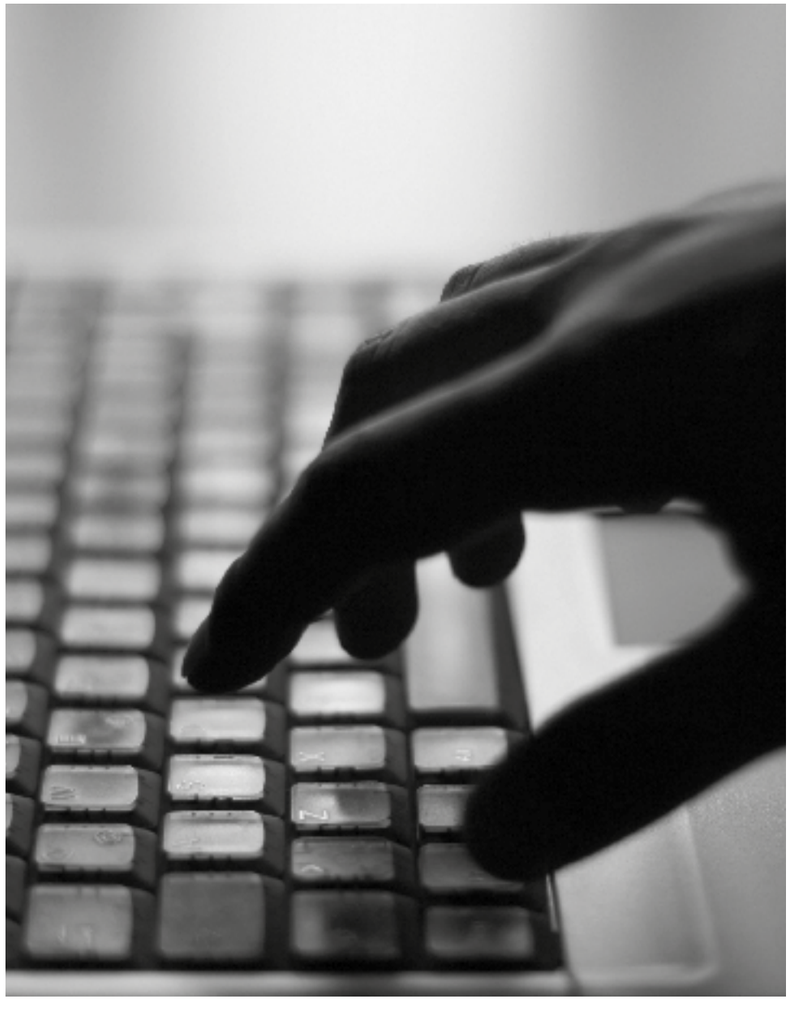
Sincere, hard-working and very wacky! (That counts as 5 words doesn't it?!?)

ABOUT THE FEATURE:

This is an interview carried out by ADISA on individuals with expert understanding on IT Asset Disposal.

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 CERTIFIED MEMBERS

UNITED KINGDOM AND REPUBLIC OF IRELAND
ADISA CERTIFIED ITAD MEMBERS

AMI Belfast	MacColl Media
AMI Dublin	Re-Tek Limited
Arrow Value Recovery (UK)	RecycleIT
AssetCare	Reuse Recycle IT Ltd
Bell Microsystems	Ricotech
BTR	S2S
Centerprise International Limited	SCC
Charterhouse Muller UK Limited	Secure IT Disposals Limited
Computer Disposals Limited (CDL)	ShP Limited
Computer Recyclers UK	Sims Lifecycle Services
E – Cycle IT Ltd	Stone Group Limited
Eco Systems IT	Tes-AMM
EOL IT Services Limited	The ITAD Works
eReco EMEA Corporation Ltd	Tier 1 Asset Management
Future Generation Disposals	Tin Global
Greensafe IT Ltd	Ultratec
ICEX Limited	

ADISA CERTIFIED LOGISTICS MEMBER

Bishopsgate
Bonds Worldwide Express Limited.

ADISA CERTIFIED SERVICE

Joyce Solutions – Migration Services.

REST OF EUROPE
ADISA CERTIFIED ITAD MEMBERS

Arrow Value Recovery (EMEA)	France
Arrow Value Recovery (EMEA)	Czech Republic
Arrow Value Recovery (EMEA)	Netherlands
Arrow Value Recovery (EMEA)	Belgium
Arrow Value Recovery (EMEA)	Germany
Diskshred (Mobile Destruction)	Germany
Alfanet S.A	Greece

UNITED STATES
ADISA CERTIFIED ITAD MEMBERS

Arrow Value Recovery (US)	Reno, NV
Arrow Value Recovery (US)	Richmond, VA
Arrow Value Recovery (US)	Dallas, TX
Arrow Value Recovery (US)	Columbus, OH
Arrow Value Recovery (US)	Hartford, CT

KOW YA, CEO OF ASVIDA® ASIA

GREEN IT: PILOTING BUSINESS GROWTH AND INNOVATION IN ASIA

With the explosion of cloud computing and 'Big Data', companies around the world are looking at ways to meet their IT infrastructure needs in the most agile and cost-efficient manner. With Asia-Pacific enterprises embracing these trends at a rapid pace, Kow Ya shares how IT asset recovery, or 'green IT' as it is commonly known, has emerged as the preferred solution for companies looking to enhance their IT asset management and transform their IT CAPEX to OPEX to create a strong competitive advantage.

According to leading research firm Canalys, the market for data centre infrastructure is poised to reach US$152 billion globally by 2016, with Asia-Pacific accounting for a quarter of this investment. Large data centres will lead this expansion, and much of such investments will be used to form the backbone of cloud and 'Big Data' services. So far, this growth has been fuelled by telecommunications and cloud service providers in China, India and other populous Southeast Asian nations where consumers are becoming more active users of social media and E-commerce, and companies are investing more heavily in data centres to analyse large chunks of information to mine consumer insights, and to provision for disaster recovery on the cloud to ensure business continuity.

Against this backdrop of burgeoning growth, IT asset recovery, a term used to describe the process of maximising the value of unused, pre-owned, or end-of-life equipment through effective reuse, is quickly becoming the preferred option for organisations today when they plan for the expansion of their data centre infrastructure.

Indeed, organisations are going through alternative and independent channels such as ASVIDAâ Asia to procure data centre equipment to balance changing business requirements, shifting technologies and budget constraints.

Says Ms Kow Ya, CEO of ASVIDA® Asia, "Where technology used to be a differentiator to a business, today it is no longer a privilege. It is very basic bread-and-butter. Every company needs to engage in some form of technology just to be on par with the rest of the competition. Against this background, IT asset recovery becomes a very natural option because it gives very attractive cost savings."

THE ASIA PACIFIC LANDSCAPE

I**n Europe and the United States,** the adoption of IT asset recovery is more widespread than Asia Pacific as enterprises have largely seen the value and benefits of adopting this practice. In these markets, IT asset recovery is a critical value creator within the IT department. While IT asset recovery is still relatively underutilised in Asia Pacific, ASVIDA® Asia foresees significant growth in this market for the following reasons:

1. COST SAVINGS

With technology moving at a relentless pace, more often than not, equipment that has been deployed and continues to function well may have been discontinued by the manufacturer. When this happens, organisations are inclined to do a technology refresh. With IT budgets shrinking, using pre-owned or new-in-box equipment, such as N-1 technology and below, provides significant cost savings of at least 30% as compared to buying equipment of the latest generation. The cost savings achieved through the purchase of pre-owned equipment can be further used to fund additional software or services, delivering greater value to an organisation. In this sense, IT asset recovery represents a form of capital conservation and optimisation for companies.

2. FREEDOM OF CHOICE

Companies, which have legacy systems that have reached end-of-life and are maintaining various heterogeneous platforms, often find it expensive to do a technology refresh. Under these circumstances, IT asset recovery offers the freedom of choice for companies to retain their legacy systems across a range of different hardware brands, and promotes greater operational stability in their IT infrastructure.

3. DISASTER RECOVERY & BUSINESS CONTINUITY

IT asset recovery has become a popular option for disaster recovery sites in a region confronted with natural disasters and political instability. Data loss and system disasters are becoming more common and costly for businesses, especially when a company does not have a disaster recovery plan in place. Instead of using brand new equipment, companies have realised that pre-owned equipment will do the trick, and are fully embracing them as cost-effective measures to keep critical systems accessible when disruptive events occur. In fact, many organisations are now relying on pre-owned equipment for parallel set-ups in their operations.

4. SHORT-TERM DEPLOYMENT

With the exponential growth in cloud computing, many service providers require short-term deployment of hardware for testing of new technologies or software. For these user acceptance testing, they are trying to find the most cost-effective way to rent and/or lease the necessary equipment, giving them the flexibility to manage changing requirements easily. IT asset recovery provides the agility and scalability that they need to roll out new projects at a much lower cost, doing away the need to invest upfront in equipment, which may not be suitable. Cloud service providers, software service providers and managed service providers, to name a few, are starting to see the value of this and are on the lookout for such solutions.

5. GOING 'GREEN'; BREATHING LIFE INTO IT ASSETS

More companies are keen to maximise their IT investments. They want to extend the productivity and useful life of technology through redeployment or remarketing. Companies, such as ASVIDA® Asia, who have the remarketing expertise to ensure that this equipment can be deployed across multiple geographies smoothly, giving financial returns related to the resale of equipment in secondary markets.

Asia Pacific is a region marked by dynamic growth. We (ASVIDA® Asia) had the foresight to recognise the potential of this business and are the pioneers of IT asset recovery in this part of the world. Already, the business is seeing strong demand from Singapore, Malaysia, Indonesia, China and India, and this is just the tip of the iceberg. IT asset recovery will continue to revolutionise how companies plan and procure their IT infrastructure, bringing more and more strategic value to businesses in this region," adds Ms Kow.

LACK OF AWARENESS AND COUNTERFEIT ISSUES POSE KEY CHALLENGES

One of the main reasons why the IT asset recovery market in the Asia-Pacific region is less mature than the United States and European markets is the lack of awareness. Enterprises in the region do not know that there is an alternative option that can help them to 'plug' hardware requirement gaps and meet the ever-changing market demand. Furthermore, there is a preconceived notion of product unreliability in a diverse region with multiple suppliers.

In certain markets, the risk of procuring counterfeit equipment is high. Language barriers and varying warranty agreements across different countries also add to the complexity of buying pre-owned equipment for companies with regional operations. This is where organisations need to exercise caution. They must be highly selective in choosing vendors or resellers that understand local business requirements and cross-border deployment of equipment, and cherry-pick those with the reputation and integrity to adopt strict guidelines in re-conditioning and testing their equipment to ensure quality control and uniformity in service delivery.

"At the end of the day, this is a business where if you know how to use it, it becomes valuable, but if you don't know how to reuse it, it has no value at all. We are talking about doing the right thing, at the right time and at the right place. And now is the time, because the Asian market is starting to become more aware of the benefits of IT asset recovery, transforming it from a 'good-to-have' to a 'must-have' in IT innovation", concludes Ms Kow.

Ms Kow Ya is the CEO and Co-Founder of ASVIDA® Asia who have more than 18 years of experience in the IT industry. She started her career at Hewlett Packard and has subsequently held various management positions that have led companies to greater levels of growth and performance. She is highly sought after for her industry insights and is frequently quoted in leading business publications in Asia. ASVIDA® Asia is a subsidiary of Procurri Corporation, a global leader in IT asset recovery and independent maintenance, with offices and a network of service coverage that extends to the U.S., Europe, Asia Pacific and Central Asia.

STEVE MELLINGS, ADISA

THE CHANGING FACE OF DATA PROTECTION

The current EU Data Protection Directive 1995 was passed into UK Law in 1998 and since then, whilst the law has stayed still, the Internet, social media, mobile working, cloud computing and a general attitude of decreasing our privacy and increasing our availability, has swept through, not only the business world, but also our very culture. In the face of this, the law, which is meant to help protect privacy of the individual, has clearly been left behind and after acknowledging this; the EU commission are currently re-writing the EU Data Protection Directive with a view of it becoming law in 2015.

It should be stressed that at this point in time – September 2014 – there are thousands of amendments still to be discussed and some crucial elements to be agreed, including whether it becomes Law rather than a Directive. There are, however, some key elements which are clear and widely expected to be approved and for the world of IT asset disposal it is essential for companies to understand these and to bring their houses into order.

INCREASED PENALTIES

There is a sea change from the regulators in terms of the powers, which they can bring to bear; currently in the UK the ICO can impose a fine of a maximum of £500,000. Eye watering to many, but to large corporates a figure they can choose to absorb should they need to. In light of this, the regulators are increasing the maximum penalties considerably with the rumours being two to five per cent of global turnover, or a maximum of £100m fine being able to be levied. Clearly these figures are not set in stone but the stick has now got much bigger!

MANDATORY BREACH NOTIFICATION

Currently, outside of the telecommunication sector, it is not mandatory to notify the data regulator of any actual breach. This results in the register of those suffering a breach being largely populated by public sector offenders, rather than in the commercial sector. This has caused much criticism of the public sector, and in particular the NHS, but it is my belief that this is a cultural issue as opposed to actual culpability. In a company governed by shareholders, where brand is key I may feel significantly less inclined to disclose a breach to the ICO unless it was so significant (Zurich 2010) or it was sure to make the press. However, this is changing, within the new act there is provision for obligatory breach notification to happen. The mechanics of this remain unclear and the crucial question of "what constitutes a breach" is also unclear, but this is further evidence of the hardening of the position of the law.

LEGAL LIABILITY FOR DATA PROCESSORS

Companies who collect ICT assets for data sanitisation services are classed as data processors when contracted to do so by a controller. Even where no contract exists, if a professional understanding is in place it could be argued that the supplier can be classed as a processor. At present there is no legal liability should these companies fail to do what they say they are doing, in other words, currently the data controller owns all of the risk. In one of the high profile breaches mentioned previously we know of commercial action being taken against the supplier by the controller, NOT by the ICO. With the new regulation the data processor will have legal liability alongside the controller.

Largely to address cloud computing this subtle but important change will see those companies who offer data processing services step out of the shadows and into the firing line. As such, in order to have your partners share in the liability a professional relationship will be required. Ad-hoc collections of "a room of old kit" won't be classed as professional. At ADISA we are already encouraging our members to engage with their customers in a far more formal way than many are expecting. This enables our members to control the engagement and effectively manage their own risk. When the law changes any company that is happy to just turn up and collect with little control is not controlling their risk and liability. This change has even be identified by the insurance sector with the first data processor insurance policy being released in September 2014.

CHANGING TECHNOLOGY

Whilst not directly relating to legislation there is a whole host of ICT initiatives, which could impact significantly on ICT disposal. Bring your own device (BYOD) brings a whole host of challenges, not least that for many users devices utilising solid state storage (SSD) would be preferable. At present with SSD there are no government-approved software overwriting products leaving the secure minded companies the option of physical destruction. The idea of seizing a leaving member of staff's own device and then

shredding it will be an interesting one for the corporate lawyers to address. Of course, ensuring that no data is stored on the device is one option, but for smart phones that is clearly not feasible. So when an employee leaves, taking their tablet or phone with them, what are your options? In order to show compliance the same controls need to be in place, as with any end of life device and thus the disposal process outlined in the previous section should apply here.

For cloud service providers', data replication and storage management make it extremely challenging to control precisely where your data is and what is happening to it. On a very basic level data is still stored on a physical device and if that storage device fails you would never know, but the question of what happens to that device remains. When engaging with the cloud, clear controls need to be put in place for many areas where security is concerned, but the addition of specific controls over the disposal of failed or refreshed hardware is essential. It would be important to also classify the cloud provider as a data processor, but as they are only responsible for hardware (in many instances) then this could be a challenge. To have data services such as sanitisation bundled with the service would allow designation of the provider to be a data processor and therefore liability would be shared with them.

DATA PROTECTION OFFICER

For businesses of a certain size, I have heard 250 or 400 data subjects being used as the entry point, they will be required to have a designated role; Data Protection Officer. This role will have express responsibility for the company's overall data protection activities and at the time of going to press, the job specification will have elements mandated by law including a guaranteed time in position making this perhaps the safest, but least desired role in many organisations!

Referring back to my author's note, assuming that the DP Officer role is given genuine responsibility and status within a business, then this could perhaps be the starting point for a change in culture within business, which could see the pace of improvement in this area accelerate.

SO WHAT SHOULD A DATA CONTROLLER DO?

For many companies compliance with law, with industry regulations, or even with their internal policies can sometimes be an opt-in and opt-out approach. The pressure of business ensures that focus is given to those areas where operations directly impact the business itself. However, with the rumoured changes to the data protection law getting more clarification and support, data protection is an area that only the brave will ignore.

For those who have data protection, information security or even brand protection within their remit, all aspects where their own company could be compromised needs to be reviewed, a risk assessment to take place and remedial actions to be enacted. One such area must be the process of ICT asset disposal as this is clearly part of the overall battlefield of information security/data protection.

In order to comply with existing legislation and to future proof against changing legislation the following (in my opinion) would be deemed as "Appropriate Technical and Organisations Measures".

- An approved means of media sanitisation encompassing all media types.
- A policy, which controls the release of these media types within all business activities.
- Internal procedures, which ensure a consistent approach to this activity, across all product sets, departments and locations and which shows adherence to the policy.
- Full asset management throughout the process and verification at each point.
- Third party contracts clearly defining the operator as the data processor and controlling any downstream processing including a strong e-waste strategy.
- Detailed and measurable specification for service delivery.
- Evidence of professional competence of supply chain, including them holding relevant industry standards and certifications.
- Management of the process through a comprehensive audit schedule.
- Reporting on the process with incident reviews, to take place as matter of course.

Of course, the pressure on business IT teams is enormous. These teams are expected to deal with more different technologies than ever before, in environments which are often out of their control. All of this with a smaller budget and fewer resources available. However, by building an intelligent ICT disposal programme along the previously suggested outlines, businesses will not only be able to show compliance with required legislation, but they will also protect their own data from exposure. Furthermore they will be able to maximise the opportunity from old infrastructure through redeployment, re-sale or donation.

Intelligent policy leads to intelligent processes and intelligent solutions. Without these elements being in place then compliance with the current and future act is clearly not evidenced and the ICT disposal process is one managed by good fortune rather than organisation control. If this is the case for your business then ask yourself, why do we bother locking the data centre door at night, what harm could possibly happen?

ADISA NEWS

ADISA PRODUCT CLAIMS TESTING IN CONJUNCTION WITH UNIVERSITY OF SOUTH WALES

ADISA is delighted to have worked with companies in both Europe and the US to help them validate claims about their products in regard to their ability to sanitise particular media types.

The results can be viewed here **adisa.org.uk/claimstesting/** but thank you to Blancco, Tabernus, IT Renew, EdR and NCS Global for participating in this scheme. More tests are underway with further exciting news on this area coming in the summer edition.

ADISA TRAINING COURSES

The ADISA industry and end-user training course have both been run within the past 12 months and now over 40 people have sat our exams. A formal review took place of both the courses and based on the feedback we have decided to create an on-line version of both of the courses. This will enable students to participate in the course in their own time rather than have to travel and take up three days from their calendar. Not only is this more convenient, but it will also keep the costs down.

Our plan is also to break the courses up more, as we covered a lot in each of the two days course. We will be able to delve into each area in much more detail, which will satisfy those who wish to know more about particular elements rather than just looking to cover lots in a course programme.

It is our ambition to have these courses live by the summer so we'll update at that point.

WELCOME TO ADISA – TONY BENHAM

ADISA welcomes Tony Benham to the ADISA staff. He joins us to initially focus on our technical auditing but also as part of the development of our research and technical capabilities. Tony has a degree in Mathematical Physics with Astrophysics from Kings College, London and was until recently a lecturer in Digital Forensics, Computer Network Security and Security Management at the University of South Wales.

Welcome aboard Tony.

SHP OPEN FACILITY IN THE US

Morecombe based ShP are delighted to announce that they have opened a processing facility in Illinois, USA. Operating with the same back office capability the processing plant is expected to be up and running within the next few months. With an initial market target of phone recovering ShP will bring their considerable expertise to the vast US market.

ARROW VALUE RECOVERY EXPAND ADISA CERTIFICATION

With their EMEA sites already in the ADISA certification scheme, Arrow Value Recovery have further committed to the ADISA programme with the addition of five of their processing plants within the US. Following a year long process which started in September 2013 with a full audit at Reno, the Arrow team have worked closely with ADISA to ensure that the formal external audit carried out in December went well and the group was approved to join the programme at Distinction level. With each and every site now on the unannounced audit rotation each Arrow site is on alert for that knock on the door from our wandering auditors.

Read the press release here.

CONGRATULATIONS AND SAFE HANDS – ALEXANDER WEST – ASSET CARE

At a time of year when most people are delivering parcels, Ali West of Asset Care made an unexpected delivery of a very special kind on Saturday 6th December.

When his wife Clare went into labour early in December it soon became apparent that they wouldn't get to the hospital in time. So with the only help to hand via the telephone, Ali and Clare brought their wonderful baby daughter into the world without the usual medical support group.

At 23.36pm, Peggy Kathryn West was delivered into the world by her brave dad (and Mum!), weighing 6lb 11oz. Congratulations to the West family.

CALL FOR SUBMISSIONS

ADISA is looking for content from both the industry and the wider end user community in the area of either data protection, information security, environmental disposal or data sanitisation. This content will be considered for inclusion within the Summer edition of this magazine. Article size is generally 600-700 words per page or for inclusion in the news section 50-100 words.

Send to **magazine@adisa.org.uk**

April 2013's edition included:

- FEATURE: Unlock the value in your IT Infrastructure
- Do you have "Skin in the Game" within IT asset disposal?

Download April 2013 here.

April 2012's edition included:

- Asset Management – Why the chain of custody fails at the asset owner site?
- Exploring the technical challenges of secure erasure on solid state devices.
- UK Data Regulator's opinon on IT Asset Disposal.
- Developing and Implementing Secure IT Asset Disposal Policy.

Download April 2012 here.

September 2012's edition included:

- Exploring the link between Cyber Crime and e-waste in Ghana.
- Ghosts from the Machines – 10 years of discarded data.
- Considerations when disposing of IT equipment – Adrian Price MOD.
- The reality of IT Asset Disposal in Asia Pacific.
- The US ITAD Marketplace.
- The Case for Business Impact Tables within IT Asset Disposal Policy.

Download September 2012 here.


ADISA