



FEATURE
THE CHALLENGE
OF GOING GLOBAL
PAGE 20

FEATURE
200 AUDITS TO SEEK IT
ASSET DISPOSAL UTOPIA
PAGE 4

9 US COMPANIES
CONTINUE TO
NEGLECT MOBILE
DEVICES SECURITY:
IMPACT ON ITAD

13 INDUSTRY
SPOTLIGHT

17 VOICE FROM
ASIA: HOW THE
INDUSTRY IN
THIS REGION IS
EVOLVING

24 BRIDGING THE
GENDER GAP
WITHIN THE IT
ASSET DISPOSAL
INDUSTRY

29 INDUSTRY
NEWS



WINNER

Education and Training
Provider of the Year

ADISA WINS EDUCATION AND TRAINING PROVIDER OF THE YEAR AT THE 2015 COMPUTER SECURITY MAGAZINE AWARDS!

REGISTER NOW FOR OUR NEW ON-LINE TRAINING PORTAL BEING LAUNCHED IN MARCH 2016



EDITORIAL AUTUMN 2015

When ADISA was incorporated in October 2010, I don't think any of us really knew what was going to unfold over the coming years. Would the industry support us? Would we get traction with Government? Would people actually value what we do? The past five years have been a steep learning curve and as we passed our 200th audit earlier on this year we've decided to be slightly self-indulgent with one of our features and published a bit of a "5 year review" written by Steve on one of his many long trips.

The remainder of the magazine focuses on different international markets. We hear from our members on a regular basis that corporates are looking for "global solutions" but they are not as appreciative of the variations in local market as they could be. We are delighted to welcome three guest authors and have permitted longer than usual pieces to help illustrate the global differences and challenges in this industry.

From the US, David Daoud provides and insightful overview of some of the challenges within the USITAD marketplace. Dr Anand Narasimhan provides an excellent commentary on the challenge of meeting multi-national customers' requirements for a global solution. And we're delighted to publish Eric Ingebretsen's piece on e-cycling in the Asia Pacific marketplace

which shows a different perspective than perhaps the US and European markets.

We change the tone a little by an interview piece by Lisa regarding the perceived gender gap within this sector. We are also delighted to publish a summary of the findings of three freedom of information request surveys undertaken over the last 12 months, the results are somewhat alarming!

As this "summer" publication will be reaching you a little later than anticipated, it doesn't feel quite as in appropriate to start discussing our next "winter" edition. With the looming change in the European Data Protection Regulation due to come into force in December we will devote our entire next edition on this change as many of the changes are extremely significant. With expert legal commentary we will explore what this means to European markets but also on a wider sphere, what does it mean to those companies doing business in Europe and moreover, what might this impact be on reciprocal privacy/data protection laws.

We hope you enjoy and please let us know your comments or requests for topics to be covered in future magazines.

Regards

The ADISA Team

EDITORS
Steve Mellings

COPY EDITOR
Paul Dalling

CONTENT AUTHORS
Steve Mellings
David Daoud
Dr Anand Narasimhan
Eric Ingebretsen
Lisa Mellings

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

EDITORIAL	2	VOICE FROM ASIA	17
200 AUDITS TO SEEK IT ASSET DISPOSAL UTOPIA	4	THE CHALLENGE OF GOING GLOBAL	20
VOICE FROM THE US	9	BRIDGING THE GENDER GAP WITHIN THE IT ASSET DISPOSAL INDUSTRY ...	24
SPOTLIGHT.....	13	FREEDOM OF INFORMATION STUDY	27
ADISA CERTIFIED MEMBERS.....	15	INDUSTRY NEWS	29



TAKING SPECIALIST DELIVERY AND DISTRIBUTION ONE STEP FURTHER

Bishopsgate provides one of the most comprehensive distribution, handling, storage and installation services available in the UK. Specialising in the transportation and assembly of sensitive electronic and medical equipment, the company has established strategically located centres nationwide to respond and cater for clients' needs quickly and efficiently.

We have continued to invest heavily in the very latest logistics machinery, transportation and training of our skilled professionals to offer the very highest standards in 2 man delivery and installation of the most fragile of goods.

Regardless of size, location or complexity, Bishopsgate are renowned for their ability to provide a fully managed, bespoke logistics solution with an unparalleled commitment to service, care and security.



Bishopsgate are the UK & Eire partner for TENESO Europe SE. This joint venture's goal is to boost competition and provide outstanding technical expertise and distribution throughout Europe. TENESO Europe SE can consistently deliver the same quality and friendly service throughout each European operation that clients of Bishopsgate have come to expect from its UK division.



Scan this code with your smartphone to jump straight to Bishopsgate!



To learn more contact us on:

+44 (0) 1793 859 010
sales@bishopsgate.co.uk
www.bishopsgate.co.uk

STEVE MELLINGS

200 AUDITS TO SEEK IT ASSET DISPOSAL UTOPIA (LOST AT COPENHAGEN AIRPORT)

As the wheels of my "executive" airline left the runway at Luton at 6.30am in April 2015 I sank into my seat, brain confuddled after four flights to three different countries in under seven days. Was I going to Copenhagen for a meeting, a presentation or a conference? Coffee would help me find the answer. On that short flight I reflected that as founder of ADISA I have put myself in the firing line for criticism as our mission at ADISA is to try to drive IT asset disposal process forward. Have we been successful? Have we made a difference? Does anyone care?



By the time we landed at Copenhagen I'd managed to write the framework for this article as I felt it necessary, perhaps for therapeutic value, to publish what the past five years of ADISA has involved and what we have learned.

The driver for starting ADISA really came about early in 2010 when I undertook 10 audits of IT Asset Disposal (ITAD) companies within the UK on behalf of a client. I was generally very shocked at what I found. Not that they were all bad (although some were), but that they were just so very different. Here was a sector (which I'd been involved in since 1999) which seems from the outside to be simple and easy and yet when viewed in a practical sense is rather more complex than many imagine. With no common standards and generic terms used as points of reference it was impossible to ascertain service quality unless a practical on site assessment was made. Even then, some of the structure of these companies left

a lot to be desired which introduced the concept of inconsistent service delivery, which of course increases risk.

At this time I met with John Sutton (ex CESG) and Daniel Smith of Blancco and we chewed over the idea of a trade association. Given their insight I spoke to several of the top companies in the sector and the feedback wasn't complementary; "It's been tried before but won't work". "The sector doesn't want to be governed, there are too many cowboys to make it work". "Customers just don't care who they use so what's the point?"

John, fresh from his CESG days, believed that regulation through standards was important and whilst the sector doesn't see it as a requirement, that will change as governance in general increases. And so we set about taking an audit document I wrote back in the late 90s and began to evolve it into something resembling a Standard. We carefully

selected a 20+ strong team of experts from all aspects of the sector including security professionals, procurement experts, asset managers, HMG as well as thought leaders from the sector itself. It would be wrong to single out any individual but there are several people who spent a huge amount of their time with me and with the Standard to whip it into shape for launch.

And launch we did, at the Blancco Partner Event in October 2010. With no government mandate, no "non-for-profit" veneer, we went to market with a bold and simple message. We're self-appointed and trying to regulate a sector which won't necessarily like us, but we feel it needs to be done. As someone who was somewhat arrogantly saying to the sector let me regulate you I thought the only way of gaining traction was to get in front of people. So with a blind belief in what I was doing and a thick skin I rolled back 15 years and hit the roads again as a travelling sales person.

I have to commend those that supported me in those very early days as the pitch was raw and value proposition completely unclear but for the early innovators they sensed that something needed to be done and with nothing else to support, perhaps ADISA was the answer.

We conducted our first audits in January 2011 and to look back now on those early audit documents is akin to looking back at pictures of yourself in the 80s – an acute feeling of embarrassment but a vague recollection that at the time it all seemed right!

Momentum began to grow and by the end of the first year we had learned a huge amount, met with many government departments and now we had seven certified sites. By the end of the second year we had 16 members and 30 the following year not to mention formal recognition from DIPCOG.

We are now nearly five years old, have certified members in seven countries and have grown to over forty certified sites. Some may view this as a success but the mission is barely started in our eyes and there is much work to be done.

So allow me to expand on what we have learnt in the past five years.....

IS THE STANDARD ANY GOOD?

The initial Standard was a fair first effort but we have refined it significantly so that we're now relatively happy that erroneous language and unnecessary criteria have been removed. For 2016 we are pulling together the regional versions of our Standard into a single document. This will prove difficult as some of the terminology, permitting and legal requirements (insurances for example) are not the same internationally. However, as the core



criteria is the same we should be able to write the Standard in such a way that a single version can be used anywhere in the world.

LESSONS LEARNT BY OVER 200 AUDITS

Oh where to begin on what has been an incredibly long journey sorting out our auditing!

In my opinion the biggest weakness in any Standard is the audit process itself. Not only is there variation in auditor competence but there is also variation in the attitude towards being audited. Some companies embrace standardisation and see it as a means for improvement where as others only really want it for a badge to use for marketing purposes.

At ADISA we started off auditing companies ourselves, John was a 27001 certified auditor, but the detractors of ADISA pointed to that as being a huge conflict of interests. So we turned to one of the worlds most recognised auditing bodies but we suffered from a lack of knowledge of the industry, a lack of understand of our Standard and also a huge variation in auditor competence. We were spending longer correcting audits than we would've done undertaking them ourselves.

And so in 2013 we were lucky enough to be introduced to Inspectorate who have a specialism in this particular sector.

Over time they have built up a good understanding of our Standard and are now able to spar properly with those companies being audited. (Tick box auditing is a pet hate of mine and unless you are able to spar with a company then how can you truly ascertain their compliance?)

At the same time in 2013 we radically changed our approach to auditing. We realised that in our third year to go and audit a company against the Standard at a prearranged date was not adding real value. What we needed was to turn up more regularly and most importantly, unannounced. So our fledgling unannounced auditing programme was designed. Professor Andrew Blyth from University of South Wales was instrumental in helping us work out how far we could push forensics on site before (a) it took too long and (b) started destroying products! With this knowledge and a recently purchased bright yellow forensic kit we employed forensic expert Frode Roarson as a contractor forensic auditor. Frode quickly picked up on the Standard and after some shadowing exercises we extended his scope from just doing forensics to include a series of operational checks. With this increased skill set we extended our audit schedule and the members were beginning to feel it. In 2014, we identified issues at around 20% of our unannounced audits with

causes ranging from minor to serious in nature.

At the end of 2014 our approach to auditing had matured to a point which allowed us to introduce our current auditing programme called "the perpetual audit programme". Each new company undergoes a Full Audit undertaken independently by Inspectorate and once approved they move onto the main programme whereby they undergo two audits per year. These could be two unannounced forensic audits or might include a full audit which is done at least every three years.

With Frode returning home we recruited another forensic scientist, Tony Benham, to the role of lead auditor. Tony has brought further expertise and control to the audit process and over the past 12 months we have identified a number of issues within the membership:

- Data remnants in partitioned areas of hard drives. (Corrective actions undertaken and research being done by ADISA into this issue.) NB. This is not meaningful data.
- Downstream shredding partners not actually owning their own shredder so shipping further downstream. (Corrective actions undertaken.)
- Complete breakdown in process control and refusal to correct within the enforced timeline. (Removal from certification scheme.)
- The use of unvetted staff. (Corrective actions undertaken.)
- Shipping of failed hard drive to repair centres. (Corrective actions undertaken)
- Shipping of non-standard

equipment to specialist processors, such as networking equipment. (Corrective actions undertaken.)

- Use of unvetted and unauthorised logistics. (Corrective actions undertaken.)
- Use of software which the customer did not approve. (Corrective actions undertaken.)

There are of course, countless wrist slapping issues which are relatively minor but still require action. Things such as CCTV camera failures, segregation or basic slipping of standards have all been identified. To the members credit corrective actions are agreed willingly and actioned quickly.

It is very important to stress here that ADISA members VOLUNTEER to go through this pain. They could leave the programme at any time and some do, either because the audit expectation is too high or because their customers don't care. The companies that remain are committed to getting it right and I'm delighted that the members are really evolving their businesses such that they deliver a consistent service EVERY time.

THE WIDER INDUSTRY ISSUES

Now, you may think that this paints the certified members in a bad light... well this brings me onto the things I've seen in the past four years from companies who either are not part of the programme or who have been removed.

- Certificates of data destruction being issued BEFORE the equipment had been processed.
- "Shredded" hard drives being wiped before being sold.
- We've seen companies go into

liquidation due to data breach but start up under a different name the next day.

- I've seen companies boxing up phones with data on, which either need repair or which are low grade and then SELL them to the highest bidder within the phone repair sector.
- I've seen equipment going through a triage process at point of receipt, the items that had a resale value being processed, the rest being boxed up and sold as a mixed WEEE consignment.
- I've seen countless proprietary software overwriting tools being used, which no evidence of any testing taking place.
- I've seen companies with "CESG" on their websites but when you go on their premises there was no evidence of approved products being used.
- I've also seen companies who have no process control in place with just pallets and shelving of assets strewn everywhere. They data wipe them (allegedly) when they sell them.

DATA CONTROLLER POOR PRACTICE.

Now, if you are a corporate employee reading this you may sit and judge the sector, "How rubbish are these companies?" or "It's a disgrace" were phrases I heard in response to a presentation I did when I explained the issues within the industry. However, while we're on the subject of bad practice here are some of the issues we see regularly from corporates.

- The release of assets without ANY

paperwork to a company with no contract and with no specification for the service to be undertaken.

- The auction of assets to the highest bidder with only a cursory specification for the data sanitisation to be undertaken.
- Inventories to be issued which are basically works of fiction and bear no resemblance to the equipment which was finally collected.
- Empty chassis collected for disposal after "all the hard drives have been removed," which were later found to contain 10 hard drives.
- Tenders coming out with lots about pricing/revenue return but NOTHING on the service to be undertaken.
- Tenders using the wrong terminology and making incorrect requests as part of the service outline.

led industry. It's happening far too slow for my liking, but ADISA members are now genuinely offering high quality data sanitisation services for their customers and, we hope!, that their customers are grateful that the huge array of risks which exist within this process are being managed appropriately.

In 2015, the EU data protection regulation changes and with that the regulating landscape. Companies will be in a panic as to how they can avoid the huge proposed fines. One piece of good news is that after five years of hard work, you can look to one security service industry and feel confident that not only are they ready and waiting for you. ADISA Certified companies have gone through the pain and hard work phase already, all you need to do is speak to them.

(Written predominately in Copenhagen airport while waiting for my return flight in April 2015. A very long day but for once on time to get home for bath and bed time stories!)

LIGHT AT THE END OF THE TUNNEL.

The ADISA team has operated now for five years, I personally have driven over 140,000 miles, we have done over 50 flights and performed over 200 audits.

ADISA is proud that we have members whose diligence towards doing it right is unwavering. Despite the pressures on margins and customers who don't seem to care, ADISA members continue to impress me with how they look to do the right thing. We have members who have NEVER had any issues identified at audit. We have new members who fully embrace the process and work their socks off to get on board and when they join they are genuinely delighted.

I feel that the world of IT Asset disposal is changing and maturing into a service



SAS offer a
**PROFESSIONAL, HIGHLY SKILLED, SECURE, COMPETITIVELY PRICED
 COLLECTION/DELIVERY SERVICE**
 that can be tailored to your request including:



Experienced professional and friendly team highly skilled in ITAD collections, datacentre removals, technical support



Company owned fleet of fully equipped, signed/unsigned secure box vehicles with anti Hi-Jack, cameras, alarms



Live Asset tracking system for customers with personal login to view collections



High security storage solutions and warehousing of your goods



Authorised Waste Carriers Licence enabling removal of WEE elements or hazardous IT



Technical capability for any degaussing, deinstalling required



Experienced professional and friendly CRB or Security-cleared drivers and technicians



Fully Managed collections Dedicated project manager and customer service team for an efficient fully managed service



24/7 collection times - Standard daytime collection, Timed collection, out of hours



Specialist installation/removal equipment

☎ 01604 870399

✉ operations@saslogistics.co.uk



DAVID DAOUD

DESPITE STATED COMMITMENT TO DATA SECURITY, US COMPANIES CONTINUE TO NEGLECT MOBILE DEVICES SECURITY: IMPACT ON ITAD

There is plenty of evidence that data security tops the minds of IT Managers and all of those tasked to administer data-bearing assets, from planning and deployment, to utilization and retirement. But there is a major gap and plenty of contradictions between stated policies and the reality on the ground. Although what keeps these Managers worried is the possibility of a data breach, which could affect their company's image, expose their organization's data to outsiders and lead to unexpected and spiraling cost, many companies still do very little to prevent breaches from taking place.



In the IT Asset Disposition (ITAD) world, securing data in theory appears to also be the number one factor in IT recycling decision making. It is often an essential reason as to why a company hires a third-party professional. If they do not hire a professional, it is also precisely because of a reported lack of trust in a third-party vendor's ability to secure data, therefore leaving the task to internal staff.

INCIDENCES OF DATA BREACH REMAIN HIGH

The instances of data security breaches during a system's life cycle abound. Serious organizations like the highly-secured US Internal Revenue Service (IRS) are not immune from data breaches. Some of these breaches end up getting some exposure in the media, like the hackers who recently managed

to access the tax return information of over 100,000 people in the United States. Last year, electronics retailer Home Depot suffered from a hacker breach that affected 56 million debit and credit cards.

Most of the breaches reported by the mainstream media are those in which hackers find weaknesses in an existing computer network or datacenter and steal information. But there is also a large number of breaches that occur through portable devices leading to major losses to consumers. The latest among such events is that of California-based US HealthWorks, which lost a laptop in April 2015 that contained information about its employees.

While the company did not disclose how many of its 3,600 employees were affected, we know the cost of cleaning up such breaches. Statistics released by Ponemon Institute on various news outlet, including NBC News (<http://www.nbcnews.com/tech/security/ponemon-institute-n364871>), calculates that this year, a data breach costs the affected company \$154 per record. Dealing with breaches is more expensive each passing year and it increased 12% this year. The Institute says the average cost of dealing with a data breach rose by a massive 23% in 2015 to \$3.79 million.

With this information in mind, what is the stance of large US companies specific to data security at the end-of-life of IT equipment? First, when it comes to the narrative, Compliance Standards' research shows that the overwhelming majority of large enterprises put data security at the top of their agenda, not only internally in the way decision making flows within the corporate structure, but also as the key metric in deciding whether to hire outside professionals and who to hire. Data security has long been the primary key deciding factor in the use of ITAD outsourcing and in defining the competitive landscape. Service providers tend to be selected often on the basis of their ability to handle data security. Of all the IT equipment types researched, only one category, the PC clients (desktops and laptops) saw cost containment as another deciding factor competing with data security. The others, namely datacenter equipment, POS/terminals, and even mobile devices (tablets and smartphones) show an overwhelming and predominant role of data security in the end-of-life process.

Over the years, the indicators of the importance of data security as a key decision factor have expanded. For instance in the datacenter, 55% of enterprises reported this year that data security is their primary reason for



hiring professionals, up ten point from 2011. In the mobile device world, that figure expanded from 39% to over 50% during that same period. In the PC client space (desktops and laptops), the jump was more modest but no less important, going from 50% to about 55%.

FOCUS ON SECURITY DUE TO REAL RISK

The focus on data security is not fortuitous. In addition to the legal requirements imposed by governments on organizations that have consumer data, companies may be facing major losses of their own confidential business assets if their data is breached. The cost of dealing with such breaches, as Ponemon calculates it, is enormous.

On the ground and in reality, US companies surveyed by Compliance Standards have plenty of reasons to worry about data security. Only 30% of the companies surveyed say they did not witness any corporate data escape or security breach. This means that a massive 70% recorded incidents of one form or another. These figures are

alarming because not only we are talking about a vast majority of companies that own consumer data, but the 70% figure is on the rise by about four points since 2011. The delta between these two periods may not represent a major statistical difference, but if anything, it shows that security issues continue to persist.

Although many, if not most, would identify "network hacking" as the leading cause of data breaches, Compliance Standards' research suggests a completely different story. In 2011, incidences of network hacking affected some 28% of the companies surveyed. This year that figure dropped to 24% owing to the investments made by companies in hardening access to their datacenters and networks. Although there are still critical vulnerabilities, the security capabilities in and around networks have improved substantially as CIOs and security chiefs beefed up their protective technologies. In the device/client space, where equipments carrying storage components are

massively and geographically distributed, the security situation has not improved at all. An alarming 48% of companies say they have witnessed loss or stolen devices. While one would expect theft to be a permanent fixture in the mobile device world, precisely given the portability aspect of these devices, the figure remains nonetheless alarming. What is also alarming is the fact that 38% say that devices were unaccounted for. They simply don't know where they are. These figures suggest that there is a substantial weakness in laptops and mobile device security and management and by extension affecting the whole IT asset management concept.

CAUSES OF BREACHES OUTSIDE OF NETWORK HACKING: SELF-INFLICTED PAIN

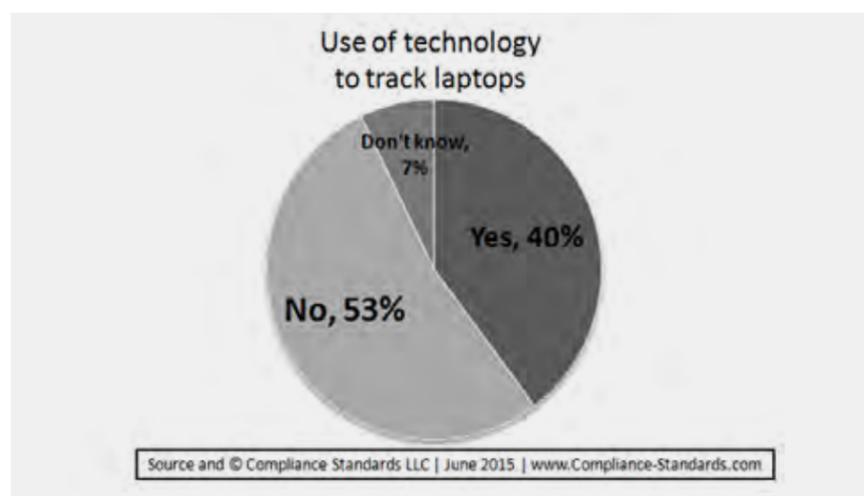
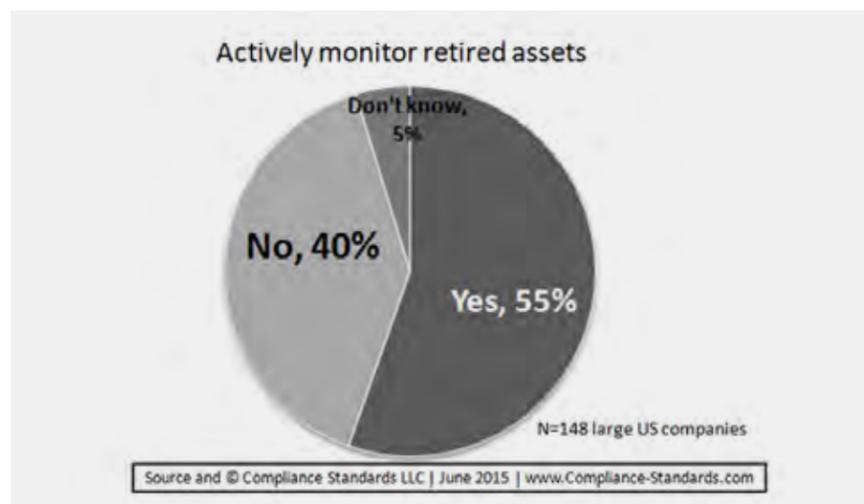
While network hacking is a phenomenon involving outside criminal elements, a great deal of data security incidences involving laptops and mobile devices occurs as a result of neglect, a sort of self-inflicted wounds. To begin with, large US companies overwhelmingly maintain an accurate inventory of corporate systems. At least 85% said they know what they own. However, mobility tends to create a curve-ball effect to corporate data security as 53% of the companies, a strict majority, do not track where their mobile devices are. So as much as they know what they own, they don't know where they are.



IMPACT ON IT ASSET DISPOSITION: OUTSOURCING RESPONSIBILITY

The inability of most US companies to track their mobile assets is problematic in that it suggests negligence and lack of proper due diligence. It is about organizations that adopt a more passive security stance rather than adopting a sound preventative data security strategy. As a result, companies tend to be more reactive to post-breach events as opposed to prevent them in the first place. The problem is not technological in nature. Tracking and remote control technologies existed for a long time. But the cost of deployment and management may be seen as too prohibitive by CXOs and the consequences are what we see today: a more lax stance vis-à-vis mobile device security.

In the ITAD world, there are many indications of IT Management wanting to shift security responsibility to their service providers. Although this stance of outsourcing risk creates demand and a market, it also creates confusion and highlights the lack of focus among large US companies. As noted earlier, data security is the primary factor driving enterprise ITAD. However, as many as 40% of the companies researched by Compliance Standards admit to not actively monitoring the process of IT asset disposition. While from a narrative perspective data security and reporting are important features of ITAD, there is still a substantial percent of US companies that maintain a distant position from the very task of a “compliant” IT recycling.



RECOMMENDATIONS AND CONCLUSIONS:

The growth of mobile devices has been phenomenal over the past 15 years with the generalization of the use of laptops and notebooks since 2000, and the acceleration of such phenomenon in 2010 with the release of the first generation of iPads. As such growth persists, involving new classes of mobile devices and wearables, opportunities for more data breaches coming from non-encrypted stolen

devices or misplaced PCs are likely to expand as well. Therefore it is imperative that organizations adopt very stringent security postures, not only during the life of the systems, but also during their final recycling phase as well. Some pointers to follow include:

- A sound strategy design begins with the recognition that corporate mobile devices are often moving around without the company's

knowing where they are exactly. While a company might have a detailed inventory of assets, knowing exactly where those assets are at any given time would provide managers with the ability to potentially recover them. There is plenty of technology that enables such asset tracking, which admittedly, remains very expensive.

- Another critical step in securing mobile devices is to ensure that the data and contents is properly locked. While disk encryption technology may not prevent hackers from entering a network, it is a good remedy against data access when an actual device theft takes place or when a system is lost. Disk encryption technology is not widely used in the corporate space, when it actually should be.
- During the disposition phase, companies are advised to monitor the data erasure techniques used and the actual business process. Often, ITAD companies use what they advertise as DoD standards involving triple erasure hard drives before they go into the secondary market. However, although we often hear the term Department of Defense (DoD) 5220-22.M Standard, this is not an officially endorsed method or standard. It was just an accepted practice of sort recommended by the Defense Security Service years ago, and then abandoned in 2007. Yet, some 33% of the companies researched by Compliance Standards utilize this so-called standard as their assets move into second lifecycle.

Another 20% use a single-pass wipe. And only 43% on the PC client front use encryption, a figure that drops below 34% for datacenters and mobile devices.

- Companies that undergo an ITAD phase must be aware of the technological changes that are affecting data storage on their devices and must research which methods are up to date. Using what many ITAD companies advocate in ways of techniques that emerged in the 1990s can be risky if newer classes of assets carry very important corporate data.
- Finally, companies need to be closely involved with reporting and understanding what their ITAD provider shares with them. Although slightly more than half of the companies researched say they monitor the reports coming from their ITAD provider, another major group neglects their obligations to check whether a vendor is doing the right thing. The involvement of the compliance and security departments in such oversight may be required to increase due diligence, as opposed to leaving all the responsibility in the hands of IT departments.

ABOUT THE AUTHOR:

David Daoud is the principal analyst at Compliance Standards, which focuses entirely on the end-of-life of IT equipment as a strategic advisor to large corporations and the ITAD industry. He has researched the mainstream IT hardware market since 1996 and expanded into hardware disposition research in 2003. In his previous role at IDC, David spearheaded the creation of IDC's GRADE certification. Since then, he has been providing consulting and expert advice to companies looking to establish best practice in their IT equipment decommissioning and helped leading ITAD service providers assess demand, understand competition, and forecast what's to come.

SPOTLIGHT ON...

LEIGH MEDHURST — CO-FOUNDER AND CEO OF FG DISPOSALS



FG Disposals has been going nearly four years now. How have you got on?

Wow, where have four years gone? Can't claim it's been easy but if you'd told me four years ago when we set the business up that we'd be where we are now I've have been very happy indeed.

Of course you're not new to the sector. What was your background before this?

I've been in this industry about 10 years now but prior to that I had a very different background in Geology and Environmental management. I moved into IT integrated solution sales and then found my way into the IT asset recovery sector. With my background I felt that the whole area of IT asset disposal was an area of significant environmental concern and also a relatively new and immature area which should be one where growth will take place.

What's surprised you about setting out on your own?

The biggest surprise was that there wasn't more surprises! Myself and Dan were thinking about our own business for some time and so we put a proper plan in place and ensured we had a strong support network around us. I can't say it's been easy but I firmly believe that if you do things right, and you do all the things you say you do, then you'll win business!

What's the biggest challenge for FG in the market?

It's probably the same as everyone else. Clients still want something for nothing and don't appreciate that we have costs to cover and with the commodity and product pricing dropping significantly our ability to charge for our service is paramount to our survival. Customers

don't really understand the second user market and still feel that their old equipment is worth lots of money when the reality is very different. I also think they don't really understand all of the subtle processes which are required to manage their assets in a professional way. Every asset has to be tracked and processed with a full audit trail to enable them to meet their own governance needs. The testing and preparation for re-use is critical AND time consuming. All of this costs money and we're constantly battling to justify our service fees.

What's your frustrations about the industry?

The industry itself is frustrating as heck. There are far too many companies who make claims which are impossible to comply with and no one is checking. The good companies in the industry do a great job providing services for their customers all under the ever watchful ADISA auditors, but there are still countless numbers of organisations who are selling on price alone without any evidence to support their claims. This is making it really hard for companies who incur costs by doing things right to cover those costs. So where will that lead us to? Will all business cut their costs and operate the same basic functional models leaving huge opportunities for process failure and therefore data breach? OR will companies understand that data destruction is a key part of the overall data protection piece and pay more attention to the vans that take away terabytes of their data?

I also think the perception of our industry is bad. We're often called the "bin men" and treated dismissively by others within the IT sector and also our customers. And yet we're guys who

manage far greater risk that the vast majority of IT service companies and the work required to do that is surprisingly complex. I think we'd like a bit more respect and appreciation and I know that has to be earned, but I would challenge any end user or IT Service Company to look at what we do and I think they will be presently surprised.

Do you think Government is doing enough?

It's getting better but ultimately no. The soon to be in place EU Data Protection Regulation may help companies move Data Protection up their agenda but I'd like to see far greater government motivation through regulatory action or more prescriptive guidance.

Something which would really help is to make dealing with Government organisations easier. The whole tendering and framework process is poor for our sector. We're only able to bid as a subset of either a whole waste management piece (including furniture etc) or as part of a wider IT services framework. When you consider the record ICO fines as a result of poor disposal you would've hoped that central procurement strategies would put in place service requirements which would help stop bad sourcing decisions being made. Sadly, it's always about price not service.

Any predictions for the industry over the next three years?

I think it's going to get much tougher within this sector. The resale market has changed significantly recently and we're not going to be able to sell just through trade as much as we do. I think we'll need to move closer to the users to get the best margins and maintain our ability to invest in our businesses.

I think from a service side customers are getting more savvy and I think you'll see a move to more on-site data destruction services and, hopefully, a greater assumption on the services they expect from their suppliers.

The quantity of equipment is going to reduce both in a numeric sense and also weights. This is going to make it impossible for those companies who cover their costs just on resale or recycling revenues to sustain their business. As a sector we should demand to be paid for our services or basically we're going to kill ourselves.

What do you do to get away from work?

I don't often get much time away from work to be honest! With an 11-month old daughter I tend to spend most of my spare time with her and my wife. Away from that I play the odd round of golf but as all of those self-employed people know, you're never too far away from the phone or laptop!

To finish off, describe yourself in three words.

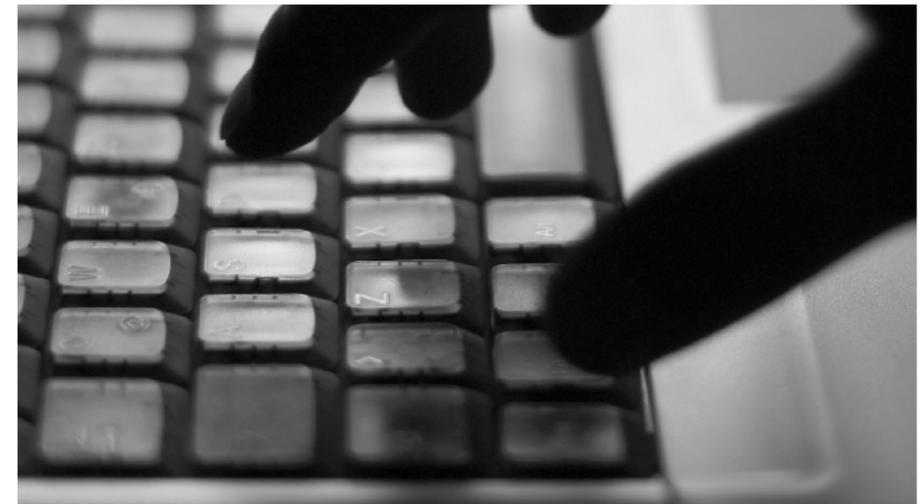
Persistent, focussed and honest.

ABOUT THE FEATURE:

This is one of a series of interviews 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

AMI Dublin

Arrow Value Recovery (UK)

AssetCare

Bell Microsystems

BTR

Charterhouse Muller UK Limited

Computer Disposals Limited (CDL)

Computer Recyclers UK

Eco Systems IT

EOL IT Services Limited

eReco EMEA Corporation Ltd

Future Generation Disposals

Greensafe IT Ltd

ICEX Limited

MacColl Media

Re-Tek Limited

ADISA CERTIFIED LOGISTICS MEMBER

Bishopsgate

Bonds Worldwide Express Limited

RecycleIT

Ricotech

S2S

SCC

Secure IT Disposals Limited

ShP Limited

Sims Lifecycle Services

Stone Group Limited

Tes-AMM

Technimove

The ITAD Works

Tier 1 Asset Management

Tin Global

Ultratec

**SEARCH FOR A CERTIFIED COMPANY HERE:
WWW.ADISA.ORG.UK/CERTIFIED-MEMBERS**

ADISA CERTIFIED SERVICE

Joyce Solutions – Migration Services

REST OF EUROPE ADISA CERTIFIED ITAD MEMBERS

Alfanet S.A	Greece
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

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



ERIC INGEBRETSEN, TES-AMM

IN OUR REGULAR FEATURE ON IT ASSET RECOVERY IN ASIA, ERIC INGEBRETSEN OF TES-AMM GIVES US HIS INSIGHT INTO HOW THE INDUSTRY IN THIS REGION IS EVOLVING

Use the words “used electronics” and “Asia” in the same sentence and images of Guiyu, nestled in China’s main manufacturing zone, immediately come to mind. We have all seen the images of children climbing over piles of electronics and workers burning or using acid baths to extract metals. Those examples are visually shocking and in places like Guiyu where that has been a reality, it has significant repercussions for the environment and workers.

Making things worse, in places like Guiyu much of this material is illegally imported under United Nations conventions as there is a specific ban on electronic waste being transferred from developed countries like the United States to countries like China and Vietnam. The Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and Their Disposal, is an international treaty that was designed to reduce the movements of hazardous waste between nations, and specifically to prevent transfer of hazardous waste from developed to less developed countries.

The good news is when you think about a geography as massive as Asia, sites like Guiyu are increasingly the exception rather than the norm. Rather it is a large informal market that absorbs the majority of used electronics using predominantly manual processing methods. The informal market creates employment for thousands of people in poverty and creates other sets of challenges as they are largely unregulated and the processing is typically not performed to more international standards. This is true of both eWaste recycling as well as IT Asset Disposition (ITAD) practices with the latter having significant impacts on the quality of the material making it to the secondary market and more

importantly the security of the data resident on storage devices.

That is not to minimise the challenges in Asia, as those challenges are significant. According to the United Nations University, globally humans generated 41.8 million metric tons of used electronics in 2014 and repurposed less than 14 percent of it. That included 6.3 million metric tons of screens and 3 million metric tons of small ICT equipment. By 2018, the amount of used electronics is expected to surge 21 percent, to 50 million metric tons driven by higher sales of devices in developing countries and shorter lifespans. Asia is expected to contribute close to 60 percent of this. Those are big numbers and Asia is a major player in the process; it is also big business. According to Allied Market Research, used Information Technology assets generated US\$2.4 billion in 2013. That number is expected to reach US\$9.8 billion by 2020. Asia is the largest revenue-generating region, accounting for US\$1.87 billion in 2013 and expected to reach US\$8.1 billion by 2020.

So there are massive amounts of material being handled by an informal market and aggregate revenues are in the billions. That recipe typically leads to concerns of corruption and irresponsible

processors. Compounding those challenges are the lack of consistent legislation across many Asian countries and the lack of adoption of standards like ADISA, R2, or eStewards.

In Europe there are umbrella regulations like the WEEE Directive that regulates much of the recycling material to ensure it is tracked and processed in a responsible manner. Recently the European Union increased the proposed fines in the case of data breach to 100 million euros or 5% of total revenue. Included in this effort are proposed changes to the EU General Data Protection Regulation (GDPR) that will require organisations to retain erasure records in the event of an investigation. In the United States, commercial and social pressures have made R2 or eStewards a key requirement for businesses and governments looking for ITAD/Recycling services. Additionally HIPAA, the Gramm-Leach-Bliley Act, FACTA, and some Securities and Exchange Commission rules all have components that speak to data privacy/protection and associated enforcement.

Conversely in Asia, while legislation exists in countries like China, South Korea, Vietnam, the Philippines, Japan, India, and Taiwan, that legislation many times is relatively weak or more often not strongly enforced. This generally



is a function of priorities as there are more pressing social and economic issues in many of these countries. On the certifications front, standards like ADISA, R2, and eStewards historically have not been widely recognised outside the OEM community and a few of the larger service providers like TES-AMM. Governments and businesses in Asia often did not see the business case for these standards or are dealing with more basic reverse logistics management issues. Interestingly enough, the same could be said of the United States ten years ago.

It would be unfair to characterize Asia as the wild west of ewaste or ITAD, but it is certainly a market that is still maturing. And as with all markets, it will mature and there are many encouraging signs pointing to that:

- Legislation in South Korea, Japan, and Taiwan have evolved to producer takeback schemes that demand OEMs recycle up to 75% of their annual production. Vietnam introduced a similar law on January 1, 2015.
- High-end datacentres are exploding across Asia to meet cloud computing demands. The complexity, security requirements, and value of the

enterprise assets coming out of those datacentres demands a very formal solution.

- In China, the regions of Tianjin, Taicing, Ningbo, Taizhou, and Zhangzhou have built local recycling parks in which informal laborers work under standard production and pollution policies. In Guiyu, the government held informal workshops to drive changes like replacing coal-fired grills with electrical heaters when taking out components from circuit boards.
- There are 19 sites in Asia that have been R2 certified (TES-AMM was the first and operates five of those sites). This expansion has largely been driven by the OEM community as they look to drive global consistency to reduce complexity and cost and by providers like TES-AMM that have embraced international best practices and recognized standards.
- OEMs are getting more engaged at the local level by providing consumer return options and helping found programmes like the Vietnam Recycling Platform, a consortium that takes back used electronic products to ensure

they are recycled in a responsible manner.

- Formal service providers of scale like TES-AMM are stepping up to meet the growing ewaste and ITAD demands of the region. There are significantly more service providers now than even five years ago and that trend will likely continue.
- Multinational corporations headquartered in Europe and the US are driving their footprint in Asia to have global consistency across environmental and data security standards. This is happening quickly; TES-AMM is privileged to have significant relationships in this space and can attest to the fact that most already either have strict controls in place or are actively moving in that direction.

Over time to continue this momentum, the Asian market will need to shift from being largely informal to being more formal. There are encouraging factors pushing the market in this direction like a greater awareness of international standards, social drivers to handle the material responsibly, surging demand for rare earth minerals used in the manufacture of electronics, and the growing recognition of the value

of functional units in the secondary market. Ultimately the shift to using formal service providers like TES-AMM will require two significant steps:

- 1) a change in mindset where there is a higher value placed on compliance and brand protection than revenue and convenience.
- 2) More legislation and significantly strong enforcement.

Signs are pointing to this shift in being inevitable and the question is becoming

more “when” than “if.” History is a guide for us here, look at any market that has evolved since the industrial revolution and you can see the parallels. Think about the global progress in the last 15 years in terms of developed/recognised standards, legislation, OEM engagement, formal service providers evolving to fill market needs, market and social level awareness, globalisation, and more. When you are living it, it always feels like a glacial pace, but in the larger sense this shift is happening very quickly right in front of us. We all

have a responsibility to participate in pushing this forward in Asia and TES-AMM is proud to be one of the leaders in that effort.

BIOGRAPHY

In his current role Eric is responsible for leading strategic initiatives for TES-AMM in North America. His efforts are concentrated on developing partnerships and overall business expansion opportunities. Prior to joining TES-AMM, Eric spent 10 years in senior management positions with Intechra and Arrow Value Recovery. During that time he focused on building/executing strategic marketing plans, integrating acquisitions, and developing and supporting Fortune 500 companies and Original Equipment Manufacturers.

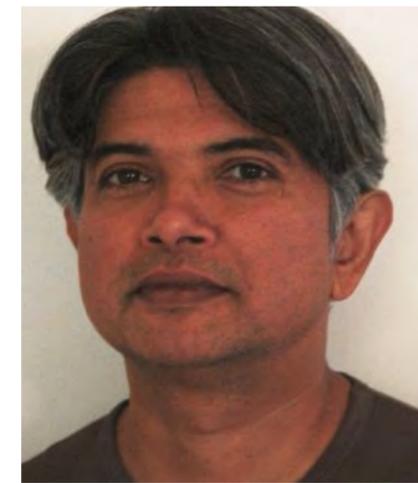
Eric has held variety of marketing, customer service, sales, and PMO leadership roles across industries that include telecommunications, aerospace, and reverse logistics. His adaptability and collaborative approach in a changing marketplace provides a valuable skill set that allows him to meet customer needs and stakeholder expectations.



DR ANAND NARASIMHAN, DIRECTOR IT ASSET DISPOSAL SERVICES, SRS EU & INDIA

THE CHALLENGE OF GOING GLOBAL

“We don’t want just a local solution, we want global”. All too often a procurement specialist will sit in offices in a major western city and place expectations on his supply chain which are just impossible to comply with. In the world of IT Asset Disposal the maturity of regional markets varies dramatically leading to very complex solutions being required in order to manage “global” clients.



DR ANAND NARASIMHAN, DIRECTOR IT ASSET DISPOSAL SERVICES SRS EU AND INDIA, GIVES HIS UNIQUE INSIGHT INTO MANAGING CLIENT EXPECTATION AND DELIVERING GLOBAL SERVICES.

It is well acknowledged that launching international IT Asset Disposal services is a long, hard process; it is even harder to do it well. Successfully delivering a quality, compliant and consistent global service is truly challenging.

In today’s interconnected world more and more businesses serve global markets, taking advantage of the change to operate in regions of the world that previously could barely be imagined. The ever-increasing amount of international commerce brings with it increasing requirements for IT asset management and disposal further and further afield.

Navigating international variances in legislation, customs, culture and values

can prove tricky for companies with data and equipment across the globe. These companies are increasingly looking to ITAD providers to navigate these stormy seas on their behalf. Amongst the many ITAD providers claiming to provide standardised global services, only a small few are getting close to a genuinely global service and none have achieved complete standardisation as yet.

RISK AND OPPORTUNITY

The current information security landscape focuses largely on managing and protecting data through life, concentrating on secure firewalls and hacking deterrents, but according to research, 70% of data breaches come from offline computers, usually after they have been disposed of by the equipment owner (Ponemon Institute’s 2013 Cost of Data Breach Study: Global Analysis). Little attention is given to managing end-of-life hardware, as the topic seems to lack the glamour of its information security counterparts.

These statistics clearly demonstrate that international organisations need to ensure that they pay attention to their end of life processes when considering their information security needs. Lack of profile for IT Asset Disposal services can introduce risk in an area where a little attention and investment can truly minimise the risk of a data breach. The potential costs of corporate information ending up in the wrong hands or equipment being illegally exported or landfilled make the

investment of time, effort and money in proactively managing end of life IT assets worthwhile.

There is no doubt that the opportunities are also there for companies willing to make the commitment to delivering global services. The global eWaste challenge is significant, and we can only truly address this if organisations take the global leap.

One study estimates that only 12.5% of global eWaste is recycled (US Environmental Protection Agency 2015), and only a tiny proportion of that will be reused. The UN Environmental Programme (UNEP) reported in May 2015 that up to 90% of the world’s electronic waste, worth nearly \$19bn (£12bn), is illegally traded or dumped each year. Innovative and forward-thinking companies can help to address these problems and have a share of a huge opportunity at the same time.



WORK IN PARTNERSHIP

EXAMPLE

“To demonstrate an example of where this is important I’ll share a scenario where my organisation was engaged to deliver services in a region with somewhat volatile political circumstances. For us to tell that client that things would be simple and straightforward would have set false expectations. Agreeing to work to the set timings of our Service Level Agreements already in place in the UK, US and Europe would have no doubt resulted in service failure, disappointment and ultimately jeopardised our trust and relationship with our client.”

“Our approach was to share openly the known risks with our client, our concerns about the unknown risks relating to the changing circumstances in that country and our options for approaching the challenge of ensuring that their end of life equipment was recovered, with data securely sanitised. Working closely with our client and their contacts within the region in question we devised a plan to deliver a new procedure, different to what we perform in other regions, but suitable for the situation and recovered the equipment successfully.”

“This activity served a pilot with a view to successfully setting up an innovative, regular, cost effective and secure service for this region. Working carefully with our client, setting realistic expectations and engaging their support in tackling the challenge resulted in a positive outcome.”

A company looking for a provider who can support them in multiple regions should listen to the supplier who is open and honest about the challenges that international service delivery presents. The company that says it’s easy is setting false expectations. Delivering a global project depends upon trust, openness and good communication between client and supplier. That trust can only be built on honesty from the very beginning of the relationship.

ADOPT A STRATEGY OF STANDARDISATION AND ADAPTATION

Companies delivering global services should have established a strong foundation of standardisation; a baseline criteria of standards which must be met in all regions in which it operates. These minimum acceptable principles form the backbone of a robust and reliable service offering.

A level of standardisation can avoid escalating operating costs and mitigate risks as well as providing a customer service which is consistent and meets their needs. ITAD companies should strive towards operational excellence to enable delivery of streamlined, efficient and cost effective services.

Continual technological development will ensure that areas such as reporting, online portals and management systems can be increasingly improved and standardised. Only when service providers concentrate resources on improving and standardising processes, ensuring administrative efficiencies and cost management, will they be able to deliver consistent customer satisfaction, high quality and consistency in returns.

Adaptation is also vital to success throughout the process. ITAD companies must understand the culture of the company in which they are working

and provide adaptations to ensure that stakeholders’ needs are met; be they staff, clients, suppliers or customers. It should be remembered that adaptation is not the same as compromise. Excellent service providers will not compromise on the core elements of ITAD service provision – security, compliance and environmental responsibility.

Regardless of the blend of standardisation and adaptation implemented good service providers will be able to deliver a unified customer experience. Key to delivering this is high quality person-to-person contact and collaboration: a partnership approach.

“Recognise that global brands are delivered locally. Take the world-leading high street fast-food chain restaurant for example, walk into any premises in the world and you can expect the same unified customer experience, in the language of the country you’re in, with local adaptations. Even if a brand has global appeal customers experience that brand differently from country to country”.

ACTIVELY IMPLEMENT A GLOBAL CULTURE

Very few companies have truly global cultures – a key requirement for success on the global stage. Multinational clients will have their own global corporate cultures and should look for an ITAD partner that mirrors their own approach.

Cultural differences really do matter: labour laws, attitudes, even simple greetings. It is vital to adopt a neutral approach – never assume that one culture dominates, take time to understand the nuances of each operating region. To do

this well it is vital to have dedicated staff committed to global service delivery.

A PRACTICAL APPROACH SUPPORTS INNOVATION

Implementing and managing ITAD services globally means working across varying time zones, languages and cultures. It also means working in the developing world which can bring a whole new set of challenges. To provide services and meet client needs in these countries it is important to take a practical approach to these challenges.

Underdeveloped infrastructure and lack of sophisticated facilities in these regions will prevent the standard approach to

service delivery. First and foremost data risk levels should be defined and a range of different service options should be considered. These options need to be practical and take into account the limitations and opportunities available.

STAY ON YOUR TOES

The speed of economic and technological changes means that the right path yesterday may not work today, and could be a problem tomorrow. Solving these dynamic challenges is what separates the companies that excel from those which struggle. Good service providers have their finger on the pulse, monitoring macro and micro environmental variations to assess their

impact on service provision and taking action to deal with change.

Equipment manufacturers are constantly trying to balance new technological improvements to their products with their recyclability. This should not be wholly the responsibility of the producer. ITAD companies should work together with these organisations to improve existing processes and develop new recycling and reuse practices to drive towards a truly circular economy. Investment in research and development is crucial to stay ahead of the curve and meet the needs of the dynamic technology environment.

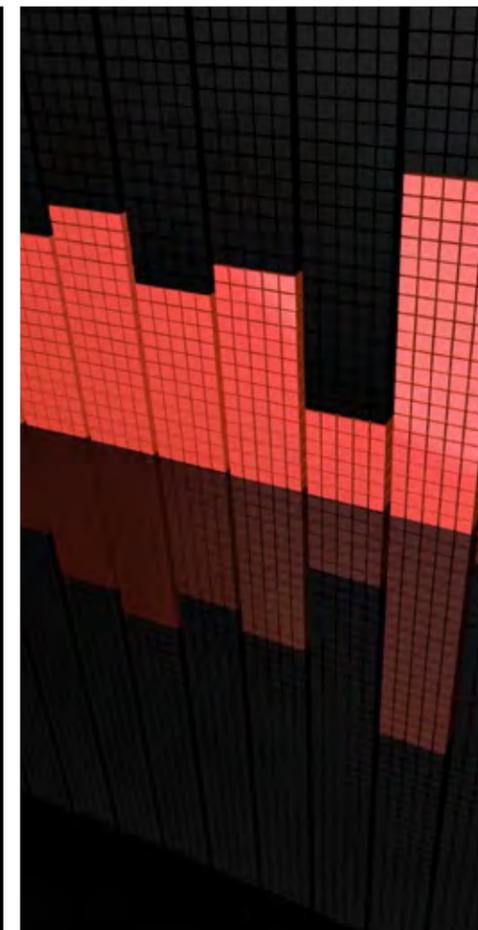
EXAMPLE

“At Sims Recycling Solutions we have delivered a variety of ITAD services across many different countries across the world and we have adapted our methodology to many challenging situations. One example demonstrating the practical tactics required in some areas was a collection of data bearing equipment from a financial institution’s base in an African nation.”

“The team arranging the collection had only limited information about the equipment or its location. Due to a lack of suitable data destruction processes in country the equipment had been placed in storage pending collection for three years. Costs and distance from our South African processing facility meant that a site survey was cost prohibitive. To tackle the challenge we consulted extensively with our client and local contacts from all parties involved and undertook the collection.”

“The environment we encountered illustrates the need for a practical, adaptive and consultative approach: many hundreds of computers were piled high in a storage area, blocking access ways, entrance and exit points and with no packing materials or organisation; no inventory of equipment was available; most equipment was broken; roadworks were taking place on the access road to the site leaving large holes in the road which was effectively a dirt track; access to the site was limited due to it being used for other purposes.”

“Many other environmental elements also impacted this collection however it was successfully completed and a process was put in place for improving services for the site going forward. The company’s vital data was protected and securely erased and the equipment was recycled in an environmentally appropriate manner – ensuring the client’s moral and legal obligations were met”.



ROLLING OUT GLOBAL CERTIFICATIONS AND STANDARDS

Any decent ITAD service provider will have in place internationally recognised certifications in ITAD processing, environmental standards and Health and Safety applying to their processing facilities in the developed world. An ITAD service provider worthy of a client's global business will have in place a plan and procedure for rolling out certifications and company standards across all their processing facilities and partner locations.

These things do have to be built over time and companies need to be creative, thinking outside the box to find sensible solutions. Things won't work the same way as they do in your home market so flexibility is important.

WHAT TO LOOK FOR IN A GLOBAL ITAD SERVICE PROVIDER

Any client looking for a company capable of delivering global ITAD services well should look for the following hallmarks of quality, experienced companies:

- Designated global service delivery personnel
- Standardised training programmes
- Standardised communication methods
- Strong Health and Safety culture and standards
- Thorough reporting and tracking throughout chain of custody
- Focus on delivering Operational Excellence
- Consistency in approach
- Defined data destruction standards and methodologies
- Internationally recognised certifications and standards and global roll out plans
- Investment in Research and Development coupled with evidence of innovation

Above all, attitude is crucial to success in this area. A partnership between client and vendor will work best when both are flexible and honest in their approach. A trusting, communicative partnership between all parties will be the foundation of a lasting and successful relationship.

Never say never, while it may seem challenging, the opportunities are there for ITAD companies to deliver global services and for clients to engage a single, effective service provider for their international needs.

LISA MELLINGS

BRIDGING THE GENDER GAP WITHIN THE IT ASSET DISPOSAL INDUSTRY

A recent report by Spring Technology states that 75% of women felt that they weren't given the same opportunities as their male counterparts in the workplace. Within the ADISA membership there are relatively few ladies who occupy places on the advisory council, which has led me to look closer to home. Whilst we feel that we, the British workplace, is an inclusive arena full of equal opportunities, is the IT disposal sector still suffering from a gender gap?



This transcript report is based on interviews carried out with several leading ladies within the sector to try to gauge what it's really like to be a professional, and a female, within the ICT disposal industry.

We thank Amanda Drinkwater (AD) of Bell Intergration, Evelyn Toma (ET) of Retek LTD, Nicola Milsom James (NMJ) of Charterhouse Muller and Stephanie Rogers (SR) of BTR for their candid insights.

LM Thanks for joining me today ladies and I'll kick off by asking the big question. Has being a woman helped or hindered your career in the IT Industry?

ET Well I felt it helped me get hired since my first employer was actively looking to recruit women with technical degrees. At that time there were very few of us around so I was very much in

demand! However, when I started my career, for the first five I would actually say being a woman was a bit of a hindrance – in particular when working with our Europe wide sales team. I felt I started from a position of having to prove myself.

AD I've worked in IT for 21 years and found being very persistent worked for me. I begged the MD of the company I was working for at the time to give me a chance. Eventually he gave in, I'm pretty sure my gender didn't have anything to do with that.

SR Going from an office environment to a virtually all male warehouse was a bit of a shock but the transition was pretty smooth. I think the industry has attracted more women into the sector recently but it still is perceived maybe from outside as a "man's world".

ET It changed for me when I turned 30. I think by that time I had proven my ability and being a woman became an advantage. For example I found it easier to diffuse serious situations with customers than maybe some my male colleagues did.

LM Is that a generation stereotypical reaction? Do the younger male members of staff see having a woman boss as completely "normal" now as opposed to 20 years ago? I have found no problem at all with the younger men in the Industry. They seem more respectful and easier to work with than maybe some of their elder counterparts.

NMJ Coming from the metallurgy and engineering industry which was totally male dominated moving into IT was more of a challenge around knowledge rather than sex. I also think that the IT we are involved in is more

about process and compliancy than the technical side of IT, so is very open to women. I never felt being a women was a hindrance.

LM I'm sure there are exceptions...I was once told to clean the loos as "you're the girl", but it is really interesting to hear that you have all found it more of an advantage being women, but then do we bring a different skill set to the table?

NJM I think we do. I think women are better communicators and excellent at multi-tasking. A woman with great time management and communication skills is a winner!!

ET I just think a mixed environment is healthier than all one sex, Women bring unique skills everywhere.

SR Being a woman actually helps when dealing with customers.

LM I agree with that. I think we have a unique blend of skills... diplomacy, multi-tasking, empathy. A good sense of humour helps especially when juggling work, family and life in general. How do you all manage with the stereotypical "career versus family" stark choice?

ET I've never seen it as a "stark" choice. I've lived with seeing less of my kids on a day to day basis than my non-working girl friends or girlfriends who made less demanding career choices. But I always tried to make up for this at weekends and holidays – and consoled myself by telling myself that I loved what I did and was giving my kids an example of living "genuinely".

SR I think some women are given a very hard decision when faced with having a family and I do think in

some cases it might hinder a career progression but I've been lucky. My wonderful daughter has just turned five and I manage to do the school run most days.

AD No I do not agree with the opinion that successful business women have to choose between their career and family. I have had four children during my career and have always managed to juggle work and home life pretty well but I am very fortunate in having a very understanding partner and being the bread winner my career has been put first.

NJM But don't you think having family gives you something to work for?

LM A sort of role model for your Kids?

NJM Exactly - I have three daughters and I think with managing my time well and with help and commitment it shouldn't mean women have to choose at all.

SR Isn't flexibility the key? I can honestly say that being a mum has not hindered my role in my business at all. I've managed to progress from FC to Owner/Director in six years and had my daughter during this time.

ET I agree that flexibility is key. When my first son was born my role involved a lot of travel so I asked to go down to four days a week. My company didn't support me initially so I offered to use a significant amount of my own holidays to demonstrate I could still do my role and achieve my goals on a four days a week basis. After I successfully demonstrated this they agreed to support it. Even so, without external support and a husband who is a great cook and actively involved with the kids

then I could not have progressed with my career in the way I did and would have felt I needed to make a "stark" choice.

AD Regardless of whether you are a man or a woman, having a family is a joint commitment so woman should definitely not be given a choice between a career and having a family.

LM So do you all think that the IT industry has become more flexible to allow women to progress and in turn that is proving to mean that career prospects are improving for women?

SR The industry definitely has more women in the field now and I certainly feel my career has improved. For women as a whole I'd like to say were now taken more seriously as more and more women become professionally qualified and gain high profile jobs throughout all industries.

ET There have been Improvements definitely. The whole idea of flexible working is much more mainstream now – and that allows woman to make choices.

AD I'm another one who thinks things have improved. Within the IT Industry things have definitely improved over the past 21 years and when I first started out there were less women in the industry. I remember going to an IT seminar in the late 90s and out of 300 delegates there were only three women!

LM That's incredible! Only three!

NJM It is but don't you think that it's women themselves that have improved it? I've seen more women competing for high level rolls and are more willing to put themselves forward so I truly think it's the attitude

of the women driving themselves that I think has changed for the better.

LM But are women now getting a better deal than their male counterparts off the back of this improvement? Are we finally starting to break through the glass ceiling at last?

AD I would definitely not say that they get a better deal as I would like to think that women get a deal equal to their male counterparts whether that is true. In reality I am not sure...

SR I'm sure there are professions out there which are still seen as "women's" roles and vice versa such as the stereotypical beautician or rig worker but I'd like to think that both sexes are branching into both; at a recent boot camp event I was actually given a full body massage by a trained fireman, who had branched into beauty too! Throughout most professions I think we're all getting pretty much the same treatment which is positive.

ET I don't believe in the glass ceiling as something imposed on women from above but more of something we have put there ourselves. I mean, in general women want a career that challenges them and fulfils them but also want to be more involved in their family in a way that a lot of men don't. As they get more senior they look upwards and see the amount of travelling and 80 hour weeks and think "That's not how I want my life to look" so they stop their career progression at the level they are at.

LM So we go back to getting the balance right and being more confident in asking for a better deal?

NJM I really don't think women are getting a better deal or even a fair deal but I do believe that they are asking for a

better deal with much more confidence.

LM Thanks Ladies and the final question...If you had the chance to do it all again what would you change?

AD Nothing – I am really happy with how I have progressed and I really wouldn't change anything.

SR Same here – I wouldn't change a thing.

ET Well I would definitely not give myself such a hard time about everything but I don't think that's a career thing!!

NMJ I would start my own company. That's the only thing I would change. I would set out exactly the same way.

So there you have it. Four successful women who have all achieved great things within the IT asset recovery sector and not one of them has found that being a woman has stopped them in any way. They have all experienced a few pitfalls along the way and the balance between family life and work life is a difficult one but these ladies have all worked out a positive way of addressing this balance.

Whilst our sample survey is small it's pleasing to hear that traditional stereotypes are not viewed by our group as being a reason why ladies cannot succeed and have a career.

Although no one is saying it is easy, but from chatting to Amanda, Evelyn, Nicola and Steph it is refreshing to see it can be done successfully!

STEVE MELLINGS

FREEDOM OF INFORMATION STUDY: NEARLY 50% OF THE POLICE FORCES ARE BREAKING THE LAW

Over the past 18 months ADISA has undertaken three Freedom of Information Studies to gauge how the UK public sector operates within the area of IT asset disposal. This article is designed to summarise those reports and to highlight evidence that a high proportion of responders are in fact currently breaking the Data Protection Act 1998.

Each FOI request included a range of questions but the key four questions relate to an awareness of the Information Commissioner's Office guidance notes and how the responders comply to these and also to the strict letter of the Data Protection Act.

We should be reminded that the current DP Act 1998 states the following:

The DPA's interpretation of the seventh data protection principle (security) requires that:

Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh (security) principle –

- a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and
- b) take reasonable steps to ensure compliance with those measures.

Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless –

- a) the processing is carried out under a contract –
 - (i) which is made or evidenced in writing, and
 - (ii) under which the data processor is to act only on instructions from the data controller, and
- b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

So we can see that any asset disposal company who performs data sanitisation services is classed as a data processor (as per the ICO asset disposal guidance notes) and therefore data controllers need to comply with the above requirements under the Seventh Principle when using those companies.

Sadly we can see that many of those companies responding are actually not complying with this legal requirement. We will pass a commentary on each question in turn.

1. Is the person responsible for ICT Disposal aware of Information Commissioner's Guidance notes for IT Asset Disposal.

	Yes	No	Other
Council	92%	3%	5%
Police	74%	7%	19%
NHS	96%	3%	1%

This is clearly the control question to gauge understanding. The high scores for Council and NHS are excellent news but low score for the police is a surprise. Of the 19% "other" score most was "unknown".

2. Do you currently have an IT asset disposal policy?

	Yes	No	Other
Council	84%	15%	1%
Police	82%	18%	
NHS	78%	10%	12%

A key principal within the ICO guidance notes is the concept of organisational control and a starting policy is necessary. The high scores of all of the responders is good but clearly a further useful piece of information would be whether or not those policies are (a) fit for purpose and (b) being adhered to.

3. Do you have a contract in place with your service provider?

	Yes	No	Other
Council	78%	18%	6%
Police	47%	47%	6%
NHS	60%	27%	13%

This is a critical part of the ICO guidance notes and as shown previously it is also listed explicitly within the Data Protection Act. So what we're seeing is that nearly 50% of police forces are not currently meeting their regulatory requirement and whilst councils and NHS fare better there is still a long way to go to show compliance to this requirement.

4. When did you last audit your partner?

A key requirement for the data controller is to take "reasonable steps to ensure compliance with their security measures." Reasonable steps have been identified by the ICO in penalty charge notices as including an audit profile. As such we can see that local councils and the police forces, by failing to audit their partners would be deemed as not showing "reasonable steps" should a breach occur. Within the Police FOI results 8% said they relied on the ADISA audits, this is precisely why we have the monitoring service in place and this could be a very quick fix for those not wishing to audit their partners.

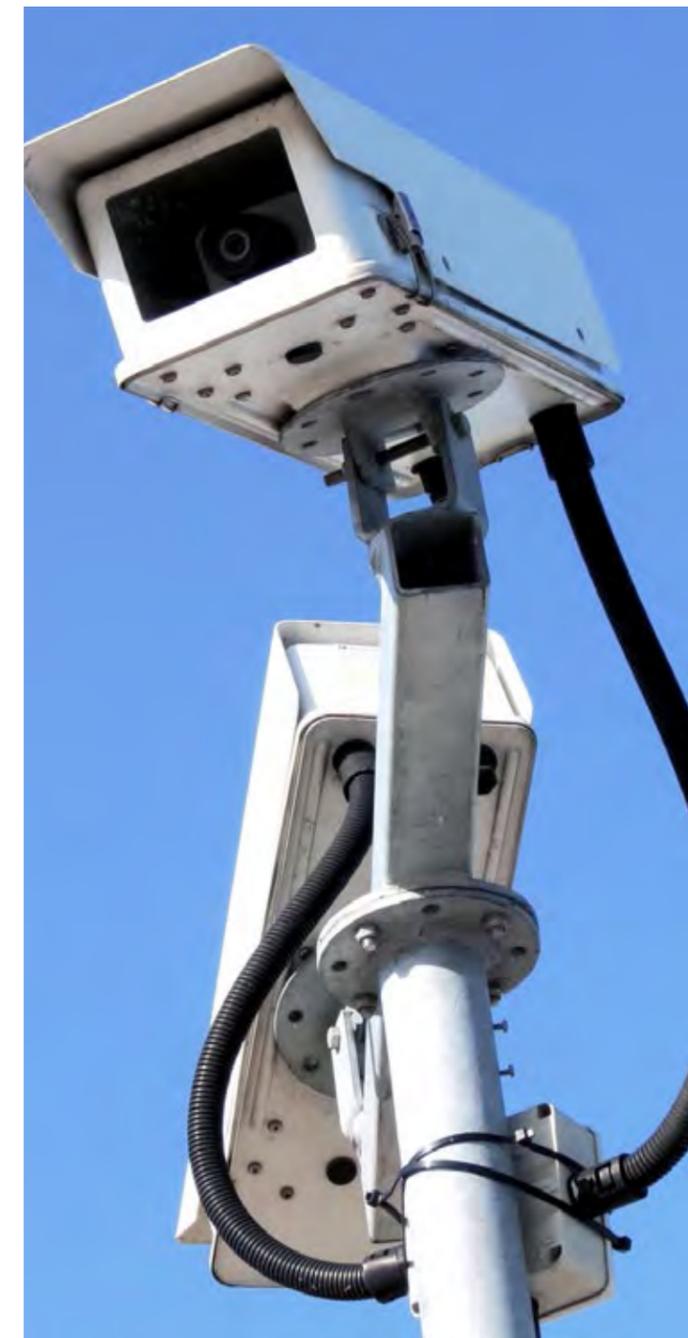
I should stress that we have total sympathy for organisations struggling to address the increasing regulatory requirements

	Within last year	Within last two years	Never	Other
Council	24%	6%	47%	23%
Police	15%	18%	54%	13%
NHS	40%	12%	25%	23%

but speaking on behalf of the sector, the frustration we have is organisations not even trying when it comes to asset disposal. Even if we ignore the legal requirements outlined above, which are not being met there are some very basic operational aspects which are being ignored. Inventories are non-existent, vendors are not selected with any degree of due diligence and in far too many cases it's the cheapest bid which wins the work. If firewalls and anti-virus solutions were selected on the same principles it would be front page news, so why is the service which is the final part of the data protection process ignored.

Of course we are biased, but many of the processes within our certification scheme are there to help data controllers meet their regulatory requirements. It's an on-going frustration from our members that they are not allowed by their customers to do the best job they can do. Sometimes down to budget but more often than not, down to apathy and a dismissive nature of the process as a whole.

For any company reading the results of these FOI studies we recommend that they take a small amount of time to query internally about how they handle asset disposal. The answers you hear, if our surveys are anything to go by, could show your currently operations to actually be breaking the law.



BLANCCO TECHNOLOGY GROUP PURCHASES TABERNUS



Hot off the press is the news that Blanco have bought their biggest competitor Tabernus. Unfortunately we don't have an inside scoop on what this means or the market strategy so as soon as we get any news we'll display on the ADISA linked in group.

Official press release here.

CDL MOVE HOME

The ADISA team wish all at CDL well in their very impressive new home. We know how much hard work you have all put into this move but we're sure it will pay off for you all.



ADISA CLOSES IN ON 250TH AUDIT

Whilst the main article features in this edition discusses our 200th audit we continue to hit the roads and are pleased to be close to our 250th. If anyone is in any doubt about what the certification means we will be doing a 250th audit campaign in November / December to answer those questions. To learn more contact lisa@adisa.org.uk

STONE GROUP WINS CORPORATE RECYCLER OF THE YEAR

Congratulations to Stone Group for being named Corporate Recycler of the Year in the MRW National Recycling Awards 2015.

During the qualifying period Stone Group recycled 1,546 tonnes of product from their recycling facility in Acton Gate. This equates to four percent of the National Target for category three of the Waste Electrical and Electronic Equipment Directive (WEEE).

In 2014, Stone Group took home the Electrical and Electronic Recycler of the Year award after demonstrating that it recycled 50% more product than it placed into the market.



EOL LAUNCH NEW HARD DRIVE SHREDDING SOLUTION - DATARAZE

To much fanfare at Data Centre World exhibition, ADISA member EOL, showcased their new hard drive shredding solution Dataraze.

Learn more here <http://dataraze.co.uk/product/>

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 next 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



Winter 2014 edition included:

- Erasing data on solid state drives
- The changing face of data protection
- Improving risk management within the NHS asset disposal process

Download Winter 2014 here.



April 2013's edition included:

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

Download April 2013 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.



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 opinion on IT Asset Disposal.
- Developing and Implementing Secure IT Asset Disposal Policy.

Download April 2012 here.

ADISA

ADISA.ORG.UK