ADISA

SEPTEMBER 2012 ISSUE 2

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

FEATURE: Exploring the links between cybercrime and e-waste

Pages 5 and 15

GHOSTS FROM THE MACHINES: 10 years of discarded data

Page 19

Images Supplied Courtesy of Davison/Greenpeace

Editorial

Documentary makers have been quick to view the plight of e-waste dumping in Africa, and other countries, as being solely an environmental disaster. Clearly, the pollution and health issues resulting from dumping e-waste in various developing countries is a very real problem which will impact not only on this generation but others to come. Thanks to the work from many agencies including the EA, BAN and Greenpeace there have been some improvements in this but the battle is far from over. There is however, an emerging acceptance that there is a second crime which is being populated by these acts, that is of data farming from discarded equipment leading to organised crime activity and attacks on the individual and businesses alike.

The theme for this edition of the ADISA magazine is "Waste and Crime" and we utilise existing articles to try to explore the hidden security vulnerability from discarded equipment and how criminals have been innovative and found ways of utilising data within the waste stream for nefarious purposes. Our heavily edited versions of these articles don't really do justice to the pieces as a whole and we recommend seeking the articles out and reading them in full.

Within this editorial I think it is important to point out that the risk of e-waste dumping and data loss CAN be managed by business end users. There is a plethora of high quality, ethical and professional companies who can recover assets, sanitise data and prepare for re-use in the correct legal way. It is the end users responsibility to find these companies, engage with them and ensure that the service expectation is one which will not promote risk taking or turns a blind eye to improper behaviour. Only by taking time and consideration in building and managing a relationship can companies be assured that their equipment is being securely managed, their data is being sanitised and their reputation is not at risk of being tarnished.

This edition is designed to give actual first hand examples of data loss and criminal behaviour caused by end users failing to focus on asset disposal in a professional and responsible way. When considering disposal it is important to understand that it is generally NOT WASTE. It is product which needs to be treated as three crucial elements; hardware, software and data. By taking time, having a policy which is fit for purpose and by engaging with the right companies, asset disposal does not need to be a black art, it does not need to be someone else's responsibility, it can be an integral part of your overall security, Corporate Social Responsibility and branding policies.

We hope the articles in this edition provoke the reader to ask some questions of yourself and your business. Enjoy.

Yours sincerely,

John Sutton and Steve Mellings
Founders, ADISA

CONTENT EDITORS
John Sutton
Steve Mellings

COPY EDITORS
Simeon de la Torre

CONTENT AUTHORS
James Warner
George Sydney Abugri
Peter Warren
Kyle Marks
Kamila Hutchison
Phil Goldsmith

DESIGN
Nick Farrar
Ben Tuckwell

PRODUCTION
Emma Craig

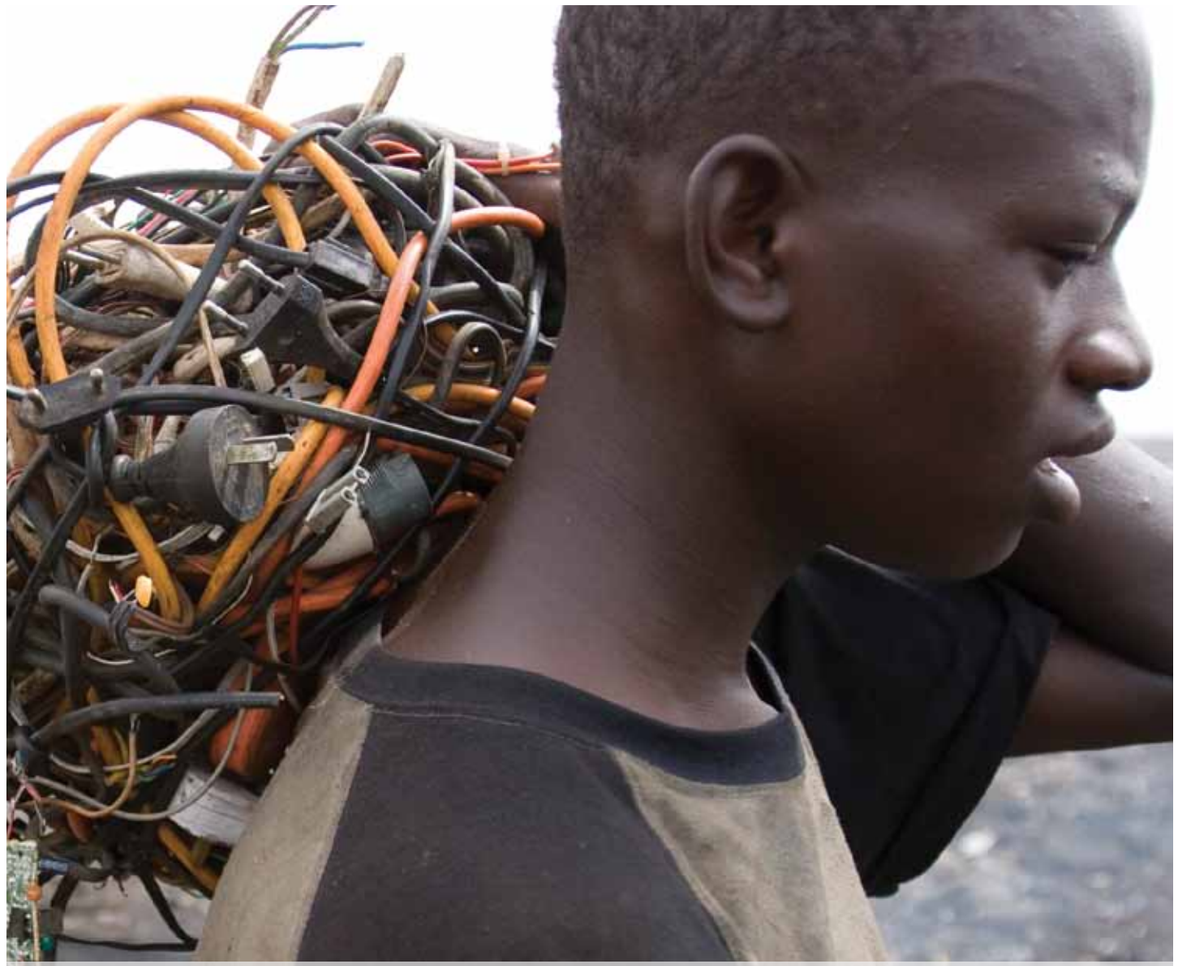
ADVERTISING ENQUIRIES
Chris Godfrey
magazine@adisa.org.uk

CONTENT ENQUIRIES
Steve Mellings
magazine@adisa.org.uk

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

CONTENTS

GHANA: Internet criminals cash in on e-waste dumping



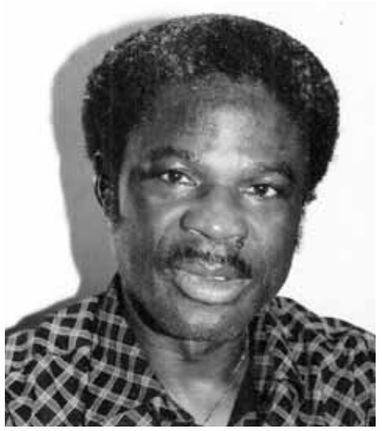
Images Supplied Courtesy of Davison/Greenpeace

There have been several studies made into data still being resident on devices sold in the electrical flea markets in Africa, but in late 2011 two articles were forwarded to us that gave first hand rather than anecdotal evidence.

This, the first of two articles in this edition, is a wonderful hands-on piece written by award winning Ghanaian journalist George Sydney Abugri. In his article he exposes first hand evidence of documented cases where fraudsters have used the landfills as a source of crucial information to ply various criminal schemes.

For the purposes of our publication, ADISA has heavily edited the original piece due to space constraints. Our edit highlights the evidence of crime being linked to e-waste landfills and it is recommended to read each piece in full to enjoy the complete story.

This is reproduced by kind permission of George Sydney Abugri. **www.sydneyabugri.com**



Award winning journalist George Sydney Abugri

Ghana holds the unenviable record as the second most Internet fraud-prone country in Africa, after Nigeria, and the seventh most cybercrime-prone country in the world. The US State Department also lists Ghana as one of the top sources of cybercrime in the world. [Source: The Global Internet Report ranking]

Award winning Ghanaian journalist GEORGE SYDNEY ABUGRI has been exploring the link between internet crimes and e-waste dumping in Ghana. Kindly reproduced under permission, this is an extract from his paper.

How a young Ghanaian resident in Accra managed to obtain sensitive personal information about United States Republican Congressman Robert Wexler and tried to blackmail the congressman remains a puzzle.

In 2011, Eric Kwame Agbosu, 27 called Wexler from Accra and told the US congressman that he had Wexler's Social Security number and other information and threatened to turn the data over to identity theft specialists if Wexler didn't pay him.

Wexler reported the matter to the United States Capitol Police who contacted the Ghana Police Service and Agbosu was traced and arrested in Accra for attempting to extort money and for identity theft.

Prior to Agbosu contacting Wexler, unidentified persons had made unauthorised attempts to gain access to the US congressman's personal bank account and to use his credit cards. It was also established that the Ghanaian had managed to obtain personal information about other prominent US citizen's apart from Wexler. The US secret service has been trying to establish how scammers like Agbosu have managed to obtain personal information about prominent US citizens like Wexler. The answer lies not in hi-tech espionage but in something far simpler.

In June 2009, an international team of investigators who arrived in Ghana to investigate the dumping of e-waste in the country accidentally established what appears to be a very strong link between the dumping of junk computers in Ghana and the epidemic of internet fraud in the country.

The investigative team was made up of Frontline/World correspondent Peter Klein and a group of graduate journalism students from the University of British Columbia who undertook a global investigation on behalf of Frontline World "to track a shadowy industry that is causing big problems around the world."

A hard drive from a discarded computer purchased from the Accra suburb at GHc 35 by the team, was found to contain confidential and sensitive details of a US$ 22 million dollar contract between the government of the United States and Northrop Grumman, one of the largest military contractors in the US. Northrop is the manufacturer of the famed Grumman Tomcat war planes. The hard drive was also found to contain defence and security contracts involving the US Defence Intelligence Agency, NASA and US Homeland Security.

Other hard drives purchased by the team, and sent to computer scientists at Regent University in Accra for immediate analysis, were found to contain what the investigators said were "intimate details of people's lives" as well as "files left on the drives by their original owners."

The files contained private financial data including credit card numbers, account information and records of online transactions undertaken by the original owners of the computers.

This investigation and the subsequent report, "Agbogbloshie in Accra, Ghana, has become one of the world's largest digital dumping grounds," has been the byword for the fight against e-waste dumping but has also exposed how innovative fraudsters have siezed the chance to create havoc on unsuspecting targets thousands of miles away.

Ghanaian computer scientist Enoch Kwesi Messiah of Regent University where some of the hard drives were sent for analysis, was quoted in a report by the investigating team as saying with the hard drives, "I can get your bank numbers and retrieve all the money from your accounts."

The team subsequently showed the hard drive containing details of the defence contracts entered into by the US government to the US Federal Bureau of Investigations in June 2009. James Durie, who is described by the investigating team as "an expert on data security for the FBI", told members of the team that he was concerned about the possible use of the information by internet fraudsters "to breach Transportation Security Administration (TSA)." According to the report, Durie said that "the government contracting process is supposed to be confidential. If I know how you're hiring the people for security related jobs, I can prepare the profile of a person to fit that model and get my guy in. Once I have my guy in, you have no security."

> Other hard drives purchased by the team and sent to computer scientists at Regent University in Accra for immediate analysis, were found to contain what the investigators said were "intimate details of people's lives" as well as files left on the drives by their original owners

Images Supplied Courtesy of Davison/Greenpeace

He reportedly said the FBI would conduct an investigation into the source of the hard drive.

Klien and his team also talked to some junk computer traders in Accra who admitted that organised criminals sometimes "comb through these drives for personal information to use in scams."

Cybercrime, or "sakawa" as it is more commonly known, is reported in Ghana weekly. Most of the victims are citizens of the United States, the United Kingdom, Germany, Australia and other countries in the west.

Ghana's Minster of Communications Mr. Haruna Iddrisu has pledged the government's determination to fight cyber fraud with all the resources at its disposal.

"The government is setting up an emergency Cyber Crime Response Team, to review existing legislature governing the Information Communication and Technology (ICT) activities and strengthen the country's cyber security. This is just part of the effort the government is making to deal with the growing Sakawa problem", Mr Haruna told police officers at a workshop on cybercrime.

The Communication Minister said Ghana's present ranking among the world's top 10 cybercrime-prone countries was "a disincentive to investment in the country's ICT sector. "

This action is commendable but with the mountains of hard drives piling up as part of the dumping of e-waste in Ghana, scammers will find it even easier to steal all the information they want for scams.

About the author:

George Sydney Abugri is a prolific, multi-award winning Ghanaian newspaper journalist. Since 1982 he has worked at Ghana's largest daily newspaper, the Daily Graphic in varied roles from reporter, through to features editor, and weekly columnist.

Abugri has been the recipient of seven {7} National Awards for excellence in journalism in Ghana. The awards include the Best Print Feature Award {three times winner}, Best Newspaper Columnist Award, Best Regional Reporter Award, Best Development Journalist Award and the prestigious Journalist of the Year Award.

INTRODUCING
ADISA IT ASSET DISPOSAL STANDARD

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

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

Launched into the UK in 2011, the ITAD standard is now being widely adopted by the leading companies in the IT asset disposal industry. These certifed companies understand the necessary elements which make IT disposal secure and are able to demonstrate this with compliance against the ITAD standard.

By using an ADISA certified company you can rest assured that your chosen partner is under constant independent scrutiny to ensure that they are protecting your data and reputation all of the time. As the recent £325,000 fine issued by the ICO for a breach within asset disposal proves - blindly trusting your provider can be expensive. ADISA certification offers you comfort that even when you aren't looking, we are.

ADISA STANDARD KEY ELEMENTS

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

THE AUDIT PROCESS

- *Full pre-audit assessment of company's capability and business ethics*
- *Annual independent audit against ITAD Standard by UKAS accredited auditors*
- *On-going spot check audits throughout the year to maintain integrity*
- *Starting in 2013 – Forensic auditing to ensure all data is removed.*

BENEFIT TO CUSTOMER

- *Confidence that your supplier has been tested by the experts.*
- *Reassurance that your supplier is constantly under scrutiny.*
- *Ability to make a sourcing decision starting from a small base.*
- *Independent vigilance via at least 3 site visits each year.*

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

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

INTRODUCING
ADISA CERTIFIED COMPANIES

CDL Computer Disposals Limited www.computerdisposals.co.uk	CONCEPT MANAGEMENT LTD www.conceptmanagementuk.com	CHARTERHOUSE MÜLLER www.charterhousemuller.com	eol IT SERVICES Sustainable, secure and socially responsible www.eolitservices.co.uk
FLECTION www.flection.com	HAMILTON ASSET MANAGEMENT XCHANGE TECHNOLOGY GROUP www.hamilton-am.com	ice Corporate IT Recycling www.ice-reuse.co.uk	FootprintMatters2u www.footprintmatters2u.com
PARTNERS IT www.partnersit.co.uk	REDEMTECH. www.redemtech.co.uk	Remploy Putting ability first www.ecycle.remploy.co.uk	re-tek www.re-tek.co.uk
SCC Technology Solutions Provider www.scc.com	scrumpymacs .co.uk serving the mac community www.scrumpymacs.co.uk	Secure I.T. DISPOSALS LIMITED www.sitd.co.uk	SIMS RECYCLING SOLUTIONS ICT ASSET RECOVERY www.simsrecycling.com
stone www.stonegroup.co.uk	tier 1 www.tier1.com	tin global The Enterprise Specialist www.tinglobal.com	ultratec Data Storage | Security | Recycling www.ultratec.co.uk

ADISA.ORG.UK

To find an ADISA Certified Company visit our website at **www.adisa.org.uk**

Within the last two to three years the press has been awash with stories of cybercrime, hacking and clandestine groups declaring war on individuals and organisations alike. As security experts work tirelessly to defend their businesses from these relatively newly organised attacks, government is stepping up and trying to help with sensible advice based on their experience of suffering these types of attack which were previously the sole remit of state sponsored agencies.

As other articles have shown, if attention is placed on trying to stop some of the lifeblood to the organisations mounting these attacks some of them may never be possible to make.

In this article, Adrian Price of the office of the Chief Information Officer for the United Kingdom Ministry of Defence explains what a security conscious organisation should consider when developing a Secure Disposal Plan and how they should treat what happens at the back door of their business as their first line of defence.

Considerations when disposing of equipment for the security conscious company

by Adrian Price, CIO – Head of Information Security Policy, Ministry of Defence

During the last three decades of the 20th century many organisations, both in the public and private sectors, embarked on a programme of digitising their paper based corporate information. As well as bringing about the obvious benefit of improved record management, it created a problem for the organisation... what had to be done to dispose of the paper mountain created by that programme? The obvious answer was to destroy it, so the mountain was invariably sent to an incinerator and all was well for the next few years.

As time moved on, the new IT systems began to fail and needed to be replaced or upgraded. Unfortunately, many organisations had failed to correctly value their information assets and identify a need for the secure disposal of those assets in their IT Through Life Management Plan, and incorporate it in the service or supply contract so it covers 'cradle to grave' asset management. This caused many a corporate or public body to hoard their equipment or the data bearing part of that equipment because they simply did not know what to do. The world had turned full circle, except this time it became a media mountain rather than a paper mountain.

So what does a security conscious organisation need to do? The answer is to write a corporate Secure Disposal Plan and ensure that the plan forms part of the IT Through Life Management Plan and future contracts for new IT systems take account of secure disposal.

The next question the security team should ask themselves is "What do I need to consider for the plan and how can I make it happen?"

The first and probably the most important element that needs to be done is an asset valuation and impact assessment. The corporate information will be an eclectic mix ranging from sensitive personal information from HR, very sensitive competitive information such as long-term planning forecasts or R&D through to relatively un-sensitive information such as out of date press releases. Once the information has been properly valued, the next step would be to identify what impact its loss or compromise would have on the organisation: this is probably the hardest step because it is a subjective judgement. For an organisation such as a central government department any information which comes into the possession of the media will be reported as top secret whether it is or not and for many corporates their position is exactly the same. One aspect of impact which is often not considered is the concept of reputational damage whereby adverse publicity in the media could cause a loss of public confidence in an organisation which in the extreme may result in a company ceasing to trade.

Having valued the information assets and identified the impact its loss would have on the organisation, the next step is to identify what would be an appropriate destruction method to mitigate against the impact which is within the organisations risk appetite and budget. There are a number of methods available which will destroy the data ranging from secure erasure, whereby the media can be reused, through to physical destruction of the media itself. Each method is not appropriate for all media types and understanding suitability must be part of the process.

It is not simply a matter of choosing an option and hoping for the best, it is still possible to recover information from media using forensic techniques depending on your threat adversary, so a judgement call is required based on the now gleaned information about the value of your information, the impact of loss of that information and also the environment where the asset is to be released to. Is it to be re-used within the same organisation or is it to be disposed of outside of the organisations for re-sale or recycling?

For this reason there are a number of destruction standards available which can help make an informed decision when selecting an appropriate method; included in these standards are BS EN 15713:2009 - Secure destruction of confidential material, DIN 66399 – Destruction of Paper, and HMG IA Standard 5 – UK Government policy document to manage risk on all storage media. In the future there will also be ISO 27040 which identifies destruction techniques for IT media. Once an appropriate method has been selected which is appropriate for the value of the information and within the organisation's risk appetite, the battle is almost over.

The next step to consider is in-house or 3rd party disposal. Unless the organisation is disposing of media in vast quantities or the organisation itself is a large distributed company who can justify the capital expenditure of erasure software, degaussers and disintegrators, the most cost effective method is likely to be through a 3rd party organisation.

There is however still one obstacle to overcome – the organisation's data controller is still liable for the data until it is destroyed, so it's not just a case of handing everything over to a 3rd party and hoping they do it properly: the security conscious organisation needs an assurance that the 3rd party they choose will do the job properly. Again this is where standards help; the ADISA Standard, launched last year, sets out the minimum criteria against which a company can be certified by ADISA. The old CCTM scheme was similar and CESG recently launched the Commercial Assurance Scheme – Destruction to replace CCTM for destruction services which has the same goals as the ADISA Standard. A security conscious organisation looking to buy in these services should consider a properly certified service rather than a company whose professional credentials have not been verified.

If the organisation has bought in a destruction service, the only thing it needs to consider is whether the destruction can be done on their premises or does the media need to be transported to a different location. If it is the former, then it's all systems go and the media mountain can be disposed of; if it's the latter, the organisation needs to develop a secure transport plan which should cover the type of vehicle used, the number of drivers, overnight stops and itemisation of containers.

To conclude; any security conscious organisation is responsible for data throughout the life of that data. In order to conclude that responsibility the data needs to be sanitised in a controlled and verified way.

The key points that a security conscious organisation needs to consider when they develop a secure destruction plan are:

- Asset valuation
- Impact assessment
- Asset reuse or destruction
- Identification of destruction method
- Secure transportation plans

Above all, the secure destruction plan needs to be incorporated in the organisations ICT Through Life Management Plan and end-of-life disposal requirements need to be written in to any contract for the supply and provision of an organisation's IT systems.

About the author:
A career Civil Servant, Adrian has been involved in the field of Information Security since 1985. Since then he has been involved in the design and development of secure systems, formal evaluations under the UK and ITSEC Evaluation Schemes and for the last 9 years has headed up the policy unit responsible for IS policy for the MoD. In addition to his policy role for the department he has been involved in the development of government IS policy. In his spare time he is a regular speaker at Information Security conferences both in the UK and overseas.

IT asset disposal in Asia Pacific

Kamila Hutchison, General Manager of Asset Management & Services at Equigroup Pty limited

Kamila Hutchison, General Manager of Asset Management & Services at Equigroup Pty limited

In a part of the world that is better known for manufacturing technology than disposing of it, Asia's ITAD market encompasses an interesting cross section of innovative remarketing organisations, through to businesses and individuals that employ the worst kind of methods to dispose of electronic waste.

Having worked in the remarketing industry for over 11 years, of which eight were spent working with ITADs across Asia Pacific, I have seen my fair share of the best and the worst.

The Australian and New Zealand markets are quite similar to Europe and the US, with some strong players who service the largest corporate and government organisations, leasing companies and vendors, along with a few smaller niche players who capture the market by specialising in a particular segment or offering unique services. There are also some players who still manage to survive even though their methods leave much to be desired. The market in ANZ is very small and ITAD's will often trade with or support each other to service clients across the vast distances.

Some US and European organisations that have set up offices across Asia Pacific & Japan are doing quite well, differentiating themselves from the local players and capturing the market of multinational corporations who aren't afraid to pay a little more for their services.

I was fortunate to have the opportunity to travel across Asia Pacific to qualify and select ITADs across 13 countries. What I quickly realised is that due to the low barriers to entry in a highly unregulated industry, anyone with a trolley and a van could market themselves as an IT disposal company and the unfortunate thing is that many customers don't know any better and keep these people in business.

I once travelled to Thailand to meet a potential remarketing partner in Bangkok. When my colleague drove me into an abandoned shopping centre I started to get worried. We walked through the mall where on each floor there were only about four or five stores that were occupied by people selling pirated software, white box computers and various electronics. We got to a store that was not too much larger than a single garage, which had piles of notebooks and desktops stacked on top of each other against the walls. I met the owner, who sat me down on a milk crate so we could have our meeting. I observed that their 'testing' bench was a small table with a screw driver and 4 point power adapter where what looked like a 14 year old boy was tinkering with a laptop he had taken apart - I couldn't wait to get out of there.

Across Asia Pacific I found much of the same thing, many remarketers were traders who were more interested in moving stock than having to touch it. Disk wiping was generally considered a nuisance, or not done at all and not many paid for recycling, if a pallet of junk could be sold for a dollar, it was. E-waste was someone else's problem. Some so-called 'recyclers' I met in Asia and even in Australia were asking more questions about the models of laptops I had for recycling than the weight of the goods, which meant that I would be paying for a recycling service and these things would likely be sold out the back door.

Illicit activity seemed like it was a constant theme of the industry. Most interesting was the lengths that people would go to in order to smuggle equipment into China. Because of the import regulations that restrict the flow of any used equipment into mainland China, a healthy black market exists thanks to the efforts of traders who work out ways to get the gear across the border. In Vietnam, people carry computers piled onto their backs and cross a river to get into China, whereas in Hong Kong, remarketing companies employ teenagers and students to catch trains all day and hand carry laptops, one at a time into Shenzhen, which can then be sold for a far greater price than in Hong Kong.

Amongst this sea of questionable characters, across the region you can however find a few truly innovative local organisations who take re-use and recycling seriously, have industry leading, quality processes, use the latest technology to extract as much re-usable material from their recycling processes and maintain a secure chain of custody when managing a client's assets. These organisations are also focused on long term sustainable growth rather than seeking short term gain, and in my travels I have often wondered why these companies aren't wildly successful, because they deserve to be.

Ultimately it is the end-user customer who decides where to dispose of their IT and electronic equipment, and there is a huge lack of awareness amongst many clients, especially those who make their selection purely on getting the cheapest price.

Apart from some major corporations, most customers in Asia Pacific don't have the same sensitivity to data privacy and environmental compliance as is seen across Europe or the United States. This allows for players with questionable motives to capitalise on the opportunities.

Until we can educate companies to make the effort to perform due diligence on their disposal partners, and they make data security and environmental compliance a key factor in the selection process, the market will continue to attract unsavory characters who cut corners and put clients, their data, and the industry at risk.

About the author
Kamila Hutchison is the General Manager of Asset Management & Services at Equigroup Pty limited and is passionate about technology, best practice asset management and educating customers on how to optimize their asset investment.

Our second feature article on the subject of "Waste and Crime" comes from James Warner, a PhD student from Harvard University. His expansive paper explores not only the criminal act itself but looks to expand into some of the underlying political and social reasons to how this has become so widespread. It is recommended to read the paper in full as space restrictions have not allowed us to cover the social commentary which is expanded upon within Jason's paper.

Reprinted with permission from the International Journal of Cyber Criminology and author, Jason Warner, Jan – July 2011, Vol 5(1): 736-749), **www.cybercrimejournal.com.**

Understanding cybercrime in Ghana: A view from below

by Jason Warner, Harvard University

Jason Warner, PhD student in African Studies and Government at Harvard University.

In January 2011, I purchased a discarded hard drive for $27 in a second-hand computer store on Bantama High Street in Kumasi, Ghana. Upon connecting it to a hard drive reader, I learned a plethora of information about the drive's former owner.

Her name is Alice (name changed). She lives in Surrey, England, just outside of London, and was a chiropractor. In 2004, she was one year away from becoming a pensioner and getting a free bus pass, a fact that made her nervous. Her Meyers-Briggs personality type is between ISTJ (energetic and analytical) and ISTP (curious and introspective), which might help to explain her regime of daily self-affirmations: "success is a journey, not a destination;" "your attitude determines your altitude." In 2005, she was also helping a family member battle through a bout of alcoholism, and as such, turned to the Bible for fortitude. Her favourite verse was Matthew 10:8, "freely you have received, freely give." (Hard drive purchased in Kumasi, Ghana, 2011).

Alice's hard drive, like so many from the United States, Europe, and Japan, are increasingly ending up in locations around the developing world after their owners have discarded their computers. While computer owners are typically assured by receptors of the machines in their home countries that their computers will be dismantled on site, such is not the case. Within the past decade, a trend has arisen that sees these old computers and other electronic devices being "discarded" into the developing world, where they are either repurposed and resold (as was the case with Alice's hard drive) or simply thrown into waste dumps out of the purview of the previous owners. This influx of electronic waste, or "e-waste," has unquestionably deleterious impacts not only on environmental and public health security of those living at importing sites, but also on the assurance of information security for both private citizens and governments from exporting sites (Warner, forthcoming).

Breaches of western information security thanks to a rise in electronic waste circulation have been particularly pronounced in Ghana, where a certain cadre of citizens has taken to searching out information on westerners' old hard drives for extortive purposes. The most recent notable case ,referred to by George Sydney Abugri, is where U.S. Congressman Robert Wexler (Democrat-Florida) was contacted by a Ghanaian, who attempted to blackmail him with information stolen from one of Wexler's discarded hard drives that had found its way to Ghana's second-hand computer market (Abugri, 2011).

In yet another recent instance, a second-hand hard drive was purchased on e-Bay that contained information on the testing procedures for the U.S. military's Terminal High Altitude Area Defense ground-to-air missile defense system, an Iraq-based operation used to shoot down SCUD missiles aimed at U.S. and ally targets (Abugri,2011). Other U.S. agency machines that have surfaced in Ghana include those from the U.S. Army, the Washington Metro Transit Authority, the State of Connecticut

Images courtesy of Jonathan Perry

Editorial comment:

It is easy to point the finger at seemingly lawless states, but it is impossible to not accept some of the blame when you consider that the feed stock for these activities is being presented to these gangs on a plate. When you add in the perilous social structure and subsistence nature of existence then perhaps the level of blame should be more proportionate to those who have options to be different than on those who feel they have none?

Mental Heath Facility, and ironically, the U.S. Environmental Protection Agency (Claiborne, 2009). Truly, for Ghanaian cybercriminals, one man's trash is another man's treasure.

Similarly, if Alice could have been an easy target for cybercrime because of the extant information on her hard drive that I purchased in Ghana, the implications for U.S. National Security because of the e-waste trade should go without saying. To this end, the United States has recently recognised the perpetration of cybercrimes as an up-and coming threat to national security. When asked about preeminent threats to the United States in a 2010 interview, Deputy Defense Secretary William J. Lynn replied: "Number one [are] the cyber threat[s]. If we don't maintain our capabilities to defend our networks in the face of an attack, the consequences for our military, and indeed for our whole national security, could be dire." As such, the new U.S. Cyber Command slated to be opened in Fort Meade, Maryland, is but one tangible example of how the U.S. is taking an active role to combat threats from information insecurity (Kruzel, 2010).

But within discussions of how to protect the United States from cyber-insecurity, no one, at least to this author's knowledge, has made the explicit recognition that the recent influx of e-waste has catalysed Ghana's status as an emerging locus of cybercrime. Indeed, this and myriad other ground-level realities often go unconsidered in discussions of cybercrime, particularly those that focus on the Global South.

About the author:

Jason Warner is a PhD student in African Studies and Government at Harvard University. He also holds an M.A. in African Studies from Yale University and a B.A. (highest honours) in International Studies and French from the University of North Carolina-Chapel Hill. He has served and continues to serve as a consultant, writer, and researcher for various national and international organisations, including the United States Department of Defense, the United Nations Development Program, Nigeria's Ambassador to the United Nations, Freedom House, CNN.com, and is also the former editor-in-chief of the Yale Journal of International Affairs.

Spotlight on...

Phil Goldsmith – Managing Director of Scrumpymacs

Phil Goldsmith, Managing Director of Scrumpymacs

Scrumpymacs (Also trades under MacFresh) is an Apple asset recovery specialist and broker.

Scrumpymacs has been going since 2007, How did you get into the business?

I was your typical sole trader broker buying and selling Thinkpads when I was offered the chance of buying a significant number of Apple xServes from Dusseldorf. Whilst we had been doing a little bit of Apple we weren't experts but when we looked into the potential residual we soon became expert!!!

In order to execute on the deal we had to raise capital from family and friends and beg people to come and help drive vans and act as porters to transact on the deal.

So you are now solely an Apple asset recovery specialist?

We do consider ourselves just as Apple specialists because we feel we can really add value through this speciality. However, some of our clients do insist on us taking all their equipment so we do still handle PC and server equipment.

Have you seen changes in the Apple market place both in terms of the technology and also the type of users over the last five years or so?

Clearly the answer to this is yes. There are two types of apple people, the "old apple user" and the "new apple user". The old Apple users were more technical, and perhaps more collaborative and viewed themselves as a niche but with the advent of the 'i' product line there is now a "new apple user" who are more mainstream and commoditised.

Within the last few years Apple has moved from being a quirky lifestyle product where there is an emotional attachment to ownership into being perceived as a genuine business enabler.

For the uninitiated, what are the main differences between Apple and a standard PC when it comes around to the time for disposing of them?

The most important thing for all our clients is that the Apple product line still holds much higher residual than the PC market. It's therefore essential to handle the product in a much more sensitive way when packaging and transporting it to ensure unnecessary damage and therefore erosion of value is minimised. For example on a typical Apple product which is 3 years old we can still return 25% of its original value to the client AFTER our costs.

It is important to note that typical brokering activities which work well for volume PC sales are not transferrable to the Apple market and greater attention to the refurbishment process is required.

In terms of data sanitisation the media used is the same magnetic or solid disk drive as you find in PCs and laptops so the process is largely the same.

Are you beginning to see tablets coming out of businesses now?

Not yet. There was not any real uptake for products like iPad 1 from the business market and iPad 2s were only sporadically used. However, we are involved in some business opportunities at the moment with a couple of corporates who are standardising on tablets as a business tool so I predict, using a standard refresh timescale, that we will see tablets coming out in greater volumes from late 2013.

Where do you feel the market will go in the next two to five years?

In terms of asset recovery, I think the clients will become more aware of the potential revenue from their disposed equipment rather than treat it as waste. This will see the disposal decision now being made with much more consideration than before and clients will want to engage with companies who can give high residual AND offer the security services required.

As previously mentioned I think we will see the tablet being used more widely in the corporate and perhaps in some installations being used instead of a laptop.

What would you like to see improved within the industry?

I would like to see greater belief and promotion of the re-use of IT assets from business users. There is now such a sense of fear of data loss that organisations are adopting a 100% risk avoidance policy and physically destroying devices. This is not only unnecessary but environmentally and financially harmful. I think greater education within the end user is required so they understand how the ITAD industry works and how best to engage with it to get the results they required.

What do you do to get away from work?

I don't really think of my business as work because I don't really do standard working hours. Being the owner I get in at 5am if there is a job to be done, but allow myself time off to pick the kids up. I value time with my three kids and wife and ensure I make time for them but, it may a cliché, I actually enjoy what I do and don't feel the need to get away from it.

That does make me sound slightly workaholic so let's add that I also play squash, cycle and I'm not unfamiliar with the inside of a pub!

To finish off, describe yourself in three words.

Driven, excitable and dedicated.

About the feature:

This is an interview carried out by ADISA on individuals with expert understanding on IT Asset Disposal. To nominate someone please email magazine@adisa.org.uk

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

This was a piece originally written and published in 2011 and reproduced under kind permission of the author Peter Warren and the Cyber Security Research Institute. The full version is available from **www.csri.info/ghosts-from-the-machines/**

The ghosts from the machines

by Peter Warren

Peter Warren, Chairman of Cyber Security Research Institute

Somewhere in the UK a young married man innocently disposed of his computer's hard drive.

The drive, which has a mix of personal data and information from the school his wife worked at, contains enough toxic information to allow the man to be comprehensively blackmailed and have his life ruined.

And as he used to work for a senior figure within the UK's Ministry of Defence, and because of some of the information on the drive this young man is a high-risk blackmail target.

Meanwhile, a major UK corporation disposed of computer equipment from one of its offices.

On a hard drive within one of these assets are the names, home addresses and mobile phone numbers of the entire staff plus other high profile individuals.

In both of these cases the hard drives on the discarded computers had not been wiped clean and still contained vital data when they were later sold.

Fortunately for both the young married man and the corporate – and by sheer chance – these hard drives came into the possession of the Cyber Security Research Institute and Glamorgan University as they carried out research on behalf of ADISA, and they were informed of the issue.

That said, they highlight once again the huge volume and value of data that is literally being thrown away by UK businesses and individuals each year.

As a result the lives of every UK citizen and detailed records of the country's businesses now haunt Britain's rubbish dumps and second-hand parts outlets – and can be readily obtained from legal internet outlets and shops by the criminal and unscrupulous.

The chance discovery of both hard drives is part of a depressing tale of continuing carelessness over the disposal of digital data that has been catalogued with remarkable ease by the researchers at Glamorgan University since February 2000 as part of their independent and ongoing disk study over a decade.

During that 10 year period the list of high profile individuals and companies whose data has been recovered simply by plugging in disks to standard computers that are readily available to any member of the pubic has been staggering: Sir Paul McCartney's bank account details on disks thrown out by Morgan Grenfell, missile secrets from Lockheed Martin, the German Embassy in Paris, Ford Motor Group, Man Trucks, Vodafone, Scottish and Newcastle, Nokia, Skandia to name but a few.

The vast amount of data discarded in this way is deeply alarming, and as a result of the refresh rate for technology and the different ways data is used, it is now increasing.

Figures show we now buy a new computer once every 4.2 years.

Due to the growing appetite for ever more powerful and feature rich mobile phones we now have a refresh rate in that type of technology which is 12 months.

The sheer range of the data thrown out is even more astounding.

During the course of the six surveys carried out since 2000, data showing criminal transactions involving billions of pounds has been found as well as drives hiding information from defence contractors, councils, health authorities, multi-national companies and ordinary members of the public.

Employee databases, personal documents, contact databases, company records, explicit emails and web searches; all emerge from the hard drives.

In many cases the information retrieved in these surveys provides potential for blackmail, in others for corporate loss, identity theft, or the effective hacking of organisations.

> If I have two machines next to each other, the one that is valuable is the one with the data on it. One machine may be able to manipulate the data better than the other but it is the data that is the raw material, and which yields all the value

So comprehensive is the information on the drives that from each survey there have been a number of arrests and criminal investigations for offences ranging from paedophilia to fraud and terrorism.

The surveys have also provoked countless company investigations into how embarrassing information made it into the public domain.

What is even more remarkable is that all of this has been possible from the analysis of just 0.0019% of the hard drives which are discarded each year.

The report carried out on behalf of ADISA estimates that the UK is now discarding 18 million gigabytes of data annually on hard drives alone, not taking into account other forms of storage devices.

So with more data being stored in different places, with widespread global hardship inspiring criminal behaviour and with an extensive list of companies already suffering in this area; why isn't the story changing?

There are signs in the last Glamorgan survey that indicate that large corporates may be attempting to deal with the issue, although the fact that none appeared in the Glamorgan data this year may simply be a question of chance.

'I would not read anything into it in terms of a growing awareness, because to see a trend emerging we will have to see it replicated a number of times and the picture is still not clear', says Professor Neil Barrett Chair of Forensics at the Royal Military College in Shrivenham.

That the results over two years have shown only minor signs of change highlights several key issues related to asset disposal.

One of these is a failure to understand the value of information itself and what it means to both businesses and individuals.

"People really seem to fail to understand that it's not the kit that's important, it's the data," says Professor Iain Sutherland, who supervised the study at Glamorgan. "If I have two machines next to each other, the one that is valuable is the one with the data on it. One machine may be able to manipulate the data better than the other but it is the data that is the raw material, and which yields all the value."

Perhaps the chief conclusion that can be drawn from the hard drive studies are that society at large is focussing too much on the technology part of 'Information Technology'. It shows less interest in the really important part – the information itself.

About the author:
Peter Warren is the Chairman of Cyber Security Research Institute which is a research centre specialising in the world of cybercrime.

He was former technology editor of Scotland on Sunday and the Sunday Express and an associate producer for BBC2, he has worked across a variety of media, including the Guardian, the Daily Mirror, Evening Standard, the Sunday Times, the Sunday Express, Sunday Business, Channel 4, Sky News, the BBC and specialist magazines.

Peter has regularly worked for over 20 years for the Sunday Times Insight team on a number of high profile investigations, he has also worked as investigations editor for Computing Magazine and Silicon.com.

The US ITAD market space

by Kyle Marks, CEO of Retire-IT

Kyle Marks, CEO of Retire-IT

The ITAD industry in the US has matured rapidly in the past few years. Media coverage has increased public awareness of the environmental problems and privacy concerns when discarded equipment is discovered in third world countries, or when confidential data falls into the wrong hands.

Environmental concerns have pushed roughly half the States and several cities to pass environmental legislation. On top of numerous Federal data security laws, a large majority of States have also enacted breach notification laws of their own. HIPAA (Health Insurance Portability and Accountability Act) receives the majority of media attention, but more than 500 various laws now affect ITAD.

Today, all leading ITAD vendors elect to become "certified" to a voluntary environmental standard, either e-Steward and/or R2. Also, every ITAD vendor claims adherence to stringent data security standards (DOD or NIST). A small but growing number of ITAD vendors have elected to become NAID certified to bolster security credentials.

While the industry has standardised and services have evolved, advances with American corporate end-users have not kept pace. Employee theft is the biggest threat to ITAD. Internal ITAD activities are often performed by low-level employees who are given little or no guidance from senior management. Few organisations have formal ITAD policies. Even fewer have formal controls in place. It is no surprise when off-network devices turn up missing.

Data security laws mandate that organisations implement "adequate safeguards" to ensure privacy protection of individuals. Organisations do a fair job of protecting systems in-use, but they fail miserably when it comes to protecting data residing on retired equipment. They are beginning to pay the price when there is a breach. Violators face increased pressure from Federal and State authorities. In addition, they incur heavy remediation costs and are being forced to defend against expensive privacy class action lawsuits.

This year, the Office of Civil Rights (OCR) began to apply unprecedented sanctions for HIPAA security violations against private companies and public agencies. In May, the OCR fined BlueCross BlueShield of Tennessee (BCBST) $1.5 million for violations following the theft of 57 unencrypted hard drives in 2009. In June, the OCR also fined Alaska's Department of Health and Social Services $1.7 million following the theft of a USB hard drive in 2009.

Significant fines following breaches may become the norm. The OCR stressed that organisations must "have in place meaningful access controls to safeguard hardware and portable devices." They "expect organisations to comply with their obligations under these rules regardless of whether they are private or public entities."

Federal agencies are not the only ones eager to punish violators. Last May, the Massachusetts Attorney General fined Boston's South Shore Hospital $750,000 following the loss of unencrypted computer tapes in 2010. The tapes were sent to a disposal vendor to be erased and recycled. But the hospital did not determine whether the disposal vendor actually had sufficient safeguards in place to protect sensitive information, among other issues.

There is no doubt that State and Federal penalties can be punitive and painful. However, the effect of a privacy class action lawsuit can be much worse. Following the loss of a backup data tape in 2011, healthcare benefits provider TRICARE was hit with eight separate privacy lawsuits, including one seeking $4.9 billion in damages. The suits allege that TRICARE and its subcontractor were negligent. TRICARE has been accused of "intentional, willful and reckless disregard of Plaintiffs' privacy," and for failing to respond to "recurring, systemic, and fundamental deficiencies in its information security."

Historically, privacy class actions falter for inability to prove recoverable damages, but this probably provides little consolation. The cost of defending privacy suits can cost millions. And, let's not forget remediation costs. In the case of BCBST, the cost of the fine was just the tip of the iceberg. In addition to the penalty, BCBST reportedly spent $17 million in investigation, notification and protection efforts.

Whether or not you are involved with the US healthcare industry, these cases draw attention to basic elements of an effective information security, especially the need for adequate safeguards pertaining to off-network and retired devices. When evaluating sufficiency of their ITAD policies and procedures, organisations must be mindful of potential administrative fines, remediation expenses, and the possibility of costly privacy class action litigation.

About the author:
Kyle is the Founder and CEO of Retire-IT. Prior to founding Retire-IT, Kyle was an executive with RetroBox, a leading IT asset disposal company that is now Arrow-Intechra. Previously, Kyle was an executive with WEGO Systems, a consultant with Bain & Company, and held numerous marketing positions with Maybelline. Kyle has a Bachelor of Arts in Economics and Business Administration from Rhodes College, and a Masters in Business Administration from Harvard Business School.

Kyle is also an IAITAM CHAMP (Certified Hardware Asset Manager Professional of the International Association of Information Technology Asset Managers).

Article 2 in the intelligent asset disposal policy series: This article is the second of five that argues the need for a five-step risk assessment methodology to be applied when determining and implementing secure disposition of redundant data-bearing IT assets.

The case for Business Impact Levels

By John Sutton

Summary of article 1: "The need for data categorisation"

The first article stated the absolute necessity for all data to be categorised (classified) as the critical first step in this risk analysis. All data, whether corporate, government or personal, must be ranked in accordance with its overall confidentiality, value and age. Consideration should be given to the effect of data aging on the confidentiality (there is a legal requirement for some data to be retained for certain minimum periods.) Figure 1 below presents a summary of these requirements.

Data aggregation must be considered when considering the business impact of data loss. Does the accumulation of a certain number of records, all at a single confidentiality level, aggregate into a higher level? Does the association of two or more separate pieces of data attract a higher confidentiality level than any of the individual data items?

Business Impact Tables

Having classified the data the next step is to determine the consequences, for the data-owning organisation, if that data was compromised. In other words; the business impact of that data loss.

In general, information security looks at three properties of data when considering potential compromise, namely;

- Data confidentiality
- Data integrity
- Data availability

Data integrity and availability are considerations when the IT asset is actually in use. For IT asset, disposal only data confidentiality is analysed for determining a risk assessment. Therefore, when assessing the effect on the organisation of a data breach, a set of business Impact Tables should be developed to assist in quantifying the legal, financial and reputational implications of a breach of data confidentiality.

Development of Business Impact Levels (BIL)

Within the UK the practice of expressing data confidentiality in terms of the impact in the business is now a common practice across public sector organisations, where most have adopted the UK government's data categorisation scheme and express Business Impact Levels (BIL) on a seven-level model (BIL0 – BIL6).

For individual organisations in any region they should decide on how many BILs best suit their business needs. SMEs may find a straight-forward three-level model of LOW, MEDIUM and HIGH meets their requirements, whereas a large national or international business could use a five-level model. The BIL table provides a framework that allows organisations to assess the BIL for compromises of the confidentiality of information and ICT systems.

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

Small companies could suffer a data loss and nobody would notice. It would be of no interest to the media in general and therefore would go undetected. So as long as a small company has backups it would suffer no long-term effects other than the need to comply with any data breach notification which may be relevant to their own region or industry.

However, the media would be very interested in large organisations, particularly any company that handles personal information such as banks or health organisations. It will make little difference to the media if the data contained no useful information, since

Data Confidentiality	Data Retention Periods			Data
	1 Month	1 Year	7 Years	
Secret		Mergers & acquisition documentation	Strategic and flotation plans	High
		Corporate bank login details		Med
				Low
Confidential				High
	Sales projections	Commercial-in-Confidence Sales data	Payroll data Client/Customer credit card and account information	Med
				Low
Sensitive			All staff members personal information	High
			Individual staff member personal information	Med
		Sales whitepapers		Low
Public				High
				Med
		Public domain data		Low

Figure 1: Data Retention Periods (Source: The Legal Ombudsman)

Business Impact Levels for an Employee					
Category	**BIL1**	**BIL2**	**BIL3**	**BIL4**	**BIL5**
Personal Finance	Minor loss of money	Major financial loss, but not involving any financial hardship	Significant loss of income, that has short term impact on way of life or causes some financial hardship	Financially devastating, e.g. personal bankruptcy or loss of home	N/A
Privacy	Loss of control of personal data beyond those authorised	N/A	Loss of control of sensitive data beyond those authorised. A compromise of identity or financial status	N/A	N/A
Health and safety	Minor injury or illness with a quick (within one week) recovery	Compromise of safety or security	Serious injury involving slight to moderate pain for 2-7 days, followed by pain/ discomfort for several weeks after 3-4 months return to normal health with no permanent disability	N/A	Permanent incapacitating injury or illness. Moderate to severe pain for 1-4. Maybe directly life threatening

Figure 2: Illustration of a Business Impact Table for an Employee

every data loss by any organisation will certainly make the headlines regardless of information concerned, potentially causing serious reputational damage.

It is only the single organisation that can determine what damage or impact that a data loss from their own organisation would cause. Some will conclude that the only need to use low levels of impact risk whilst others will consider their data is always very sensitive, and consequently will have a significant impact if such data became compromised.

Development of BIL tables

Having quantified all data in terms of a BIL, the next step is to produce impact statements that actually state the impact upon the business in the event of a data compromise. The terminology chosen for the impact statement will reflect the degree of the impact on the business or individual.

For example, the BIL table below illustrates how the factors that affect an individual employee's personal finance, privacy and health and safety should be expressed in terms of a business impact. (NB the full version of this table would also include categories for the impacts on an employee's identity and potential embarrassment or distress)."

Without a commonly agreed impact assessment tool, organisations may not be in a position to effectively share implications of a particular information risk with their partners, clients etc. With such a tool it becomes possible to communicate in a manner that allows the collaborative management of information risks.

Automating the processes for managing risk is not straightforward if the impact is not commonly understood. The separate business units in a single organisation need more clarity over the controls that may apply in their relationships. Hence with the increased importance of collaboration it is becoming more important to be able to share the implications of a risk with about the potential business impact. Organisations need to do so in a manner that is universally understood. There is no commonly agreed method available to communicate with enough detail, the impact of information risk for organisations.

One important difference to understand with BILs is that they do not measure the size of the risk event; a given information risk would not necessarily have the same business impact of each party in a collaboration. However, the ability to be able to share in commonly understood terms of what a given risk might have on all parties, allows for proper negotiation between them over the rest controls or mitigations that should be employed.

Similarly, the financial implications of a data confidentiality compromise will not always be the same for each organisation – losing £10,000 would have a very different effect on a small organisation than it would on a large corporate. It is important to ensure the BIL used reflects the true implications of a risk event for each individual organisation. Using or adopting generic BIL is a dangerous strategy unless those BIL have been mapped onto the organisation and they meet that specific organisation's own risk position.

A set of well-developed BILs in tabulated form will provide organisations with a common understanding of the resulting consequences for individuals and organisations, to aid them in performing effective risk assessments and analysis when disposing of IT assets.

The next article in the series looks at how a company can profile threats, who may be targeting their business and introduces Threat Capabilities.

The previous article is available from ADISA and can be requested by emailing magazine@adisa.org.uk.

Industry news

New CESG Assured Service (CAS) scheme launched

With the demise of the CCTM scheme many have waited to see what would come along and replace it. CESG have launched the CAS and CPA schemes which cover both products and services. Full details are best read from the official site. **http://www.cesg.gov.uk/servicecatalogue/cas/Pages/cas.aspx**

ADISA open office in Australia

In order to fulfil customer demand ADISA have opened an office in Melbourne, Australia. Based from Albert Park, this office will be run by John Hutchison of the Carmine Group and will service the Asia, Pacific Region. Website is under development at **www.adisa.com.au**

SWEEEP Kuusakoski performs Alchemy with waste TV glass

The world's first truly sustainable CRT TV glass recycling solution goes into operation this month. Historically waste CRT glass has gone back into making new CRT screens. The diminished market for new CRT screens means a solution for a global problem had to be found.

SWEEEP Kuusakoski's £2 Million investment in the first full production Nulife glass furnace is set to liberate 1kg of lead per waste CRT. The furnace is powered using SWEEEP Kuusakoski's existing 100% renewable energy supply with zero emissions and zero waste generated.

Existing customers, some from as far away as Australia, and key industry figures will be exclusively invited to witness alchemy as part of the official opening: **www.sweeep.co.uk/glassrecycling**.

Blancco are 15 years old this year!

Blancco, the global leader in certified data erasure and computer reuse solutions, is this year celebrating 15 years at the forefront of data erasure technology and management processes. From a small start-up venture in Finland 15 years ago, Blancco is today the most certified software in the industry, and the preferred erasure choice for millions of users around the world.

Mr. Kim Väisänen, CEO and Co-Founder of Blancco, says 2012 so far has been the best year yet for the company. "This year we are excited to have received Common Criteria certification, an international standard for computer security" he said. "We are proud of the fact that we have more independent third party certifications than anyone else in the industry."

Blancco's history timeline and a short video message from Mr. Väisänen can be seen on its 15th anniversary campaign site: **www.blancco.com/15-years.**

Mark Saunders now at 99 Delta

Ex Redemtech and EWS, Mark Saunders, was headhunted by 99 Delta, an IT Solutions company based in London, to oversee the design, set up and launch of a new IT disposal processing facility in Reading. Saunders, who has many years' experience within the world of IT disposal, will utilise 99 Delta's extensive client base with a view of offering high quality data sanitisation, remarketing and recycling services. Saunders said "Coming from a background where the service provided to the client was of the highest importance I was delighted when 99 asked me to put together a bespoke IT recovery service for their clients. The whole service is orientated around brining value back into the client base rather than simply collecting equipment and the plans 99 have for taking it to market are extremely exciting." **www.99delta.com/**

Richard Parker joins ICEX as Managing Director

ICEX are delighted to announce the appointment of Richard Parker as Managing Director. Not only will ICEX Ltd benefit from his wealth of commercial, services and industry experience but he understands the goals of the company and what is required to drive the business forward towards significant growth and improved performance. Parker has over 6 years of experience working within the Data Destruction and Technology Recycling industry as well as in excess of 24 years in the corporate world.

Parker says "I am relishing the opportunity of being Managing Director of ICEX Ltd and will endeavour to maintain the high standards that the company has built its reputation on, whilst growing the business at the same time. I am also very excited to be at the forefront of a business that is changing the way organisations handle data and disposal of technology assets."

Charity rally

Alex MacColl, Managing Director of MacColl Media Ltd, who operate MacKing – the second-hand Mac retailer have embarked on a 3,000 mile round trip to Naples, Italy in two old "bangers", raising money for the Motor Neurone Disease Association, in memory of Alex's aunt Cath who died in 2009. Having successfully raised over £17,000 in the past three years they are on target to add a further £6,000 this year. Those wishing to donate can do so at **http://www.justgiving.com/lancia**

ICEX sponsor charity golf day

A beautiful sunny afternoon in lush Essex was the perfect antidote for an afternoon away from work whilst doing much for a good cause. Local charity "Build a school in Gambia" has been supported by Essex based ICEX for a number of years and at an event with over 100 players, £13k was raised in the name of a good cause. Fellow Industry operators RDC and EOL also attended the golf and evening dinner.

New division at Advanced Digital Dynamics.

Advanced Digital Dynamics Limited recognised as a leading supplier of new IT and refurbished computer hardware have announced the launch of Advanced Data Destruction. Utilising extensive expertise in secure data destruction and sanitisation ADD are deploying a dedicated secure onsite data destruction and IT Asset Disposal service. Jonathan Belbin, ADD's Managing Director said to ADISA "This is an exciting time for ADD, we are now in a position to utilise our extensive re-marketing skills and network in order to offer organisations an affordable onsite data destruction solution alongside our IT support and maintenance contracts. Watch this space."

Ricoh Europe expand asset recovery operations

Ricoh Europe has announced the formalisation and expansion of its existing asset recovery program. Through the programme, Ricoh will remove customer data residing in any location on a printer or MFP including the Hard Disk Drive, NVRAM or paper trays. A Ricoh spokesperson says "It was a natural progression for us to expand our service to a fully certified cleansing of the whole Ricoh device. Our customers appreciated the high quality service they received from Ricoh so expansion of it to more Ricoh devices and across Europe made perfect sense."

The service will be introduced across Europe in 2012. Visit **www.ricoh-europe.com for more information**.

RICOH
imagine. change.

Tabernus integrates with IQ Reseller

Tabernus Certified Data Erasure has announced a strategic integration with Minnesota based IQ Reseller – an IT Reseller and Profit Management Software. Thanks to this agreement those using IQ Reseller can now manage their data security needs and take the received asset straight to market within a single tool.

It is expected that the Integrated IQ Reseller and Tabernus erasure solution will be available to European customers within the coming weeks. "Our customers in Europe can already see the benefits of using Tabernus Certified Data Erasure solutions, the IQ Reseller integration will be the missing piece of the jigsaw for a lot of companies," comments Daniel Dyer, Tabernus VP of European Operations.
www.tabernusuk.co.uk

Lombard Technology Services become the first ADISA Certified Leasing Company. The second most exciting thing to happen to their Director, Riessen Hill this summer!

During the recent audit at Lombard, their technology director Riessen Hill let it slip that he's been in the press recently. We assumed local press but from the above photo you can see that he was being far too modest.

Riessen was selected as one of 8,000 torch bearers, and his unusual torch handover made the national news. Nominated to carry the torch because of his work with Samaritans, the confidential support service, he tells us what it was like to carry the flame through the streets of Hertfordshire.

What was it like to carry the torch?
The day was unbelievable from start to finish. It was an amazing experience and so special to have so many family and friends amongst the buzzing crowd of St Albans. I wanted the 350-metre experience to last as long as possible, so I walked and jogged very slowly!

Tell us about the process of passing the flame...

When I first received the flame, I danced a very merry jig with my fellow torch bearer. When I passed the flame onto the final torch bearer, we 'knighted' one another! The security staff were extremely worried I'd set her hair alight, but my nerves held up. Snaps of these moments featured on the BBC and ITV news.

How did you come to be a torch bearer?

It was a total surprise to me as my sister, Kirsty, nominated me in secret. I felt honoured to be chosen in recognition of my work with Samaritans and really excited to be part of such a special event.

What inspired you to become a Samaritan and what does this involve?

When I hit forty, I decided that I wanted to give something back. Volunteering as a Samaritan involves one three to four hour shift a week. I offer support to people in need over the phone, by email, text or face to face. Working with Samaritans over the last few years has been incredibly rewarding.

Do you still have the torch?

Oh yes, it's a keeper – I'm far too attached to put it on eBay. We were briefly separated when it made a guest appearance at my 12-year-old daughter's school assembly and at my 7-year-old daughter's classroom show and tell.

What Games events did you get a chance to watch?

I managed to get tickets to see athletics, boxing and basketball. I was especially excited to see GB's Clare Strange in the wheelchair basketball. Clare was a fellow torch bearer with me. She broke her back in a horse-riding accident in 1997, but was playing for the GB wheelchair basketball team just one year later. Competing in her third Paralympic Games, Clare is a true inspiration.

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

Next issue – April 2013

Publication theme – Cash £££££

Feature 1: The true cost of IT disposal

- Outlining what it takes to securely collect and process an IT asset
- What is the cost of data breach?
- What is the potential cost of reputational damage?

Feature 2: Software harvesting

- What is it? What are the benefits? What are the pitfalls?

Feature 3: Commodities

- So your asset is no longer a product. Does the material have value?

[The features are subject to confirmation]

Regular features such as:

- The continuation of the "Intelligent IT disposal" article
- An interview with a leading participant within the IT disposal marketplace
- Industry news and updates
- Voice from North America
- Voice from Asia

Subscription:

This is a free of charge subscription magazine.

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

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

Article submission:

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

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

WHAT DO YOU NEED TO ERASE TODAY?

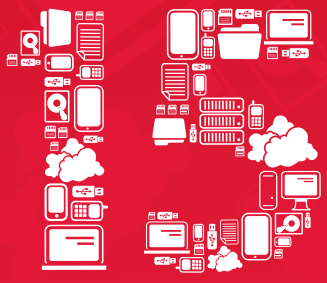
This year Blancco is celebrating 15 years as the global leader in certified data erasure

› Win one of 5 great prizes in our birthday prize draw

› Take advantage of our 15% FREE mobile edition sales offer

› Find out how Blancco can help with all of your data security needs

www.blancco.co.uk/15-years



blancco

CELEBRATING 15 YEARS

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