ADISA

WINTER 2016 ISSUE 6

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

INSIGHT
EU DATA PROTECTION REGULATION
PAGE 3

ANALYSIS
EXPLORING THE HIDDEN AREAS ON ERASED DRIVES
PAGE 17

AUDIT MONITORING SERVICE

When releasing ICT Assets as part of your disposal service it is vital to ensure your supply chain is processing your equipment correctly. This is both for peace of mind and to show compliance with the Data Protection Act and the Information Commissioner's Office guidance notes. All members within the ADISA certification program undergo scheduled and unannounced audits to ensure they meet the certified requirements. Issues that arise can lead to changes in their certified status – or even having it withdrawn. These reports can be employed by end-users as part of their own downstream management tools and are available free of charge via the ADISA monitoring service.

Subscribers to the service will automatically get updates of any changes to the ITAD's status within the ADISA program and be told of any relevant changes to the business. Updates will be sent for any of the following reasons:

- Any change in certified status both positive (improvement) or negative (audit failure).
- Any new services which have been added to the ITAD's certified status.
- Any change in credit status as per Dunn and Bradstreet.
- If they have decided to leave the program for other reasons. It is essential to clarify the reasons to ensure no reputation damage to the ITAD.
- The results of any incident reports which may have been undertaken.

To ensure fair play, any company who signs up for this service will have their contact details sent to the ITAD, which will then approve or query the reason for being monitored. They can do this by contacting the person making the monitoring request and understanding the business reason for it.

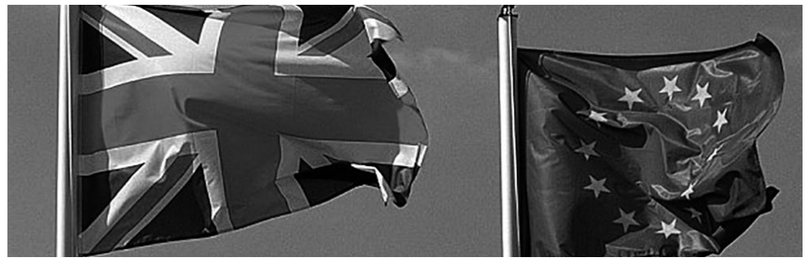
Upon agreement from the ITAD the person will be added to the monitoring list. This is to encourage only current or genuine potential customers to sign up - and avoid those seeking commercial gain. For that reason only genuine business email addresses are allowed. Those such as Hotmail are not.

TO REGISTER PLEASE VISIT WWW.ADISA.GLOBAL/CONTACT-US

For further information please contact ADISA on 0845 557 7726 or email members@adisa.global

ADISA ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

EDITORIAL WINTER 2016



This edition was due for release in the summer. But the events of June 23 were not only the stuff of debate in bars and boardrooms throughout Europe – they forced us into countless re-drafts.

Our theme for this edition is Data Protection legislation in Europe and the US and our lead feature includes a perspective on the implications of Brexit on Data Protection in the UK and also a wider European perspective on how to comply with the EU General Data Protection Regulation when disposing of redundant assets.

Jeffrey Dean explores Privacy and Data Protection regulations in the US marketplace and Tony Benham examines HPA and DCO issues with magnetic media.

Tony also gives an insight into his life as an ADISA auditor. He outlines what goes to make a good, bad or ugly audit for both the member and for him as the auditor.

We welcome external authors who wish to discuss anything that will add value to members. In this edition, Gill Barstow discusses a favourite subject of ours – building your value proposition. And an old friend, Gavin Coates, introduces his ITAD Track software which has been 4-5 years in development and is currently deployed by several ADISA members.

As we are now deep into December we would like to wish you all a very merry Christmas and hope you all have a great 2017.

We hope you enjoy - and please send us comments or requests for topics to be covered in future magazines.

Regards, The ADISA Team

EDITOR
Steve Mellings

COPY EDITOR
Richard Burton

CONTENT AUTHORS
Steve Mellings
Anthony Benham
Gill Barstow
Alan Dukinfield

DESIGN
Antoney Calvert at
Colourform Creative Studio
colour-form.com

PRODUCTION
Antoney Calvert

ADVERTISING ENQUIRIES
magazine@adisa.global

CONTENT ENQUIRIES
Steve Mellings
steve.mellings@adisa.global

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

Tel: +44 (0) 845 557 7726
adisa.global

CONTENTS

STEVE MELLINGS

EU DATA PROTECTION REGULATION

ABSTRACT ON BREXIT

The result of the referendum on June 23 was for the UK to exit the European Union, leaving UK business in a period of uncertainty with the impact on law and commerce unclear. However, where Data Protection is concerned it was clear that the UK would need to adopt comparable and equivalent legislation to the new EU General Data Protection Legislation (EU GDPR) 2016 in order to be able to exchange data with EU Member States or to qualify for a UK/EU Privacy Shield. In addition, those companies who already process EU Citizen data are obligated to comply with this legislation regardless of EU membership.

Given the timing of the potential exit, the ADISA position was that, as it became EU law on May 25, 2016, member states would have to enshrine it into their own legislative framework by May 25, 2018, a date at which the UK will still be a member of the EU. As such, we believed that EU GDPR would be enshrined into UK law before any exit took place.

Our position was ratified by The Secretary of State for Culture, Media and Sport, Karen Bradley MP, who confirmed on October 24 2016 that the UK will enshrine the EU GDPR into UK law. The UK Information Commissioner, Elizabeth Denham, confirmed the ICO's position at the same meeting. As such it seems that, despite the turmoil of Brexit, UK business is going to have to prepare and implement key processes if it is going to comply with the incoming law.

ABSTRACT ON EU GDPR

Looking back, the original EU Data Protection Directive 95/46/EC was passed in 1995 and since then the pace of change in technology has been frightening and most importantly attitudes to hardware ownership and privacy, are evolving at an even quicker rate. Cloud did not exist and the Internet of Things was not even thought possible. This new law makes significant strides forward in regard to current technology and changing habits but also to try to give greater control back to the data subjects themselves.

In April 2016 the new EU GDPR, was finally agreed and became enforceable on 25 May 2016. This piece of legislation is the most significant amendment to European Data Protection or privacy law since the original Directive 95/46/EC was passed. With many companies already struggling to protect their data, their ability to show compliance to this new regulation is in doubt.

Whilst "regulation fatigue" may indeed be real for an organisation, the new data protection regulation sets a bench mark out that organisations will ignore at their financial and reputational peril. The document itself is some 200 pages long containing over 74 articles so for the purposes of this article let's look at the most important elements and relate them to the data processing service of asset disposal.

There is some good news for companies faced with this burgeoning responsibility. The solution for one part of data protection, end of life asset disposal and data sanitisation, is already in place. This paper reviews the law changes in terms of data processing activities and overlays how the existing ADISA Certification programme can help companies meet their regulatory requirements.

The target audience for this paper are organisations who dispose of ICT assets and look to protect their businesses from suffering data breach during this process and to create a compliant position with EU GDPR. Within those organisations the paper should be read by any person in a role with a data protection oversight, in compliance or relevant operational role.

In addition, the paper is targeting ADISA certified members to enable them to see how their certification can help their customers meet their regulatory responsibilities.

EU DATA PROTECTION REGULATION 2016 ARTICLES RELEVANT TO ASSET DISPOSAL

The EU General Data Protection Regulation 2016 was passed into European Union law in May 2016 and with each member state having two years to enshrine it into their own national law, should be taken as the bench mark piece of legislation which organisations need to review when considering data protection.

This legal document is extremely in-depth and includes many core concepts that won't be covered in this paper. What follows is the identification of critical parts of this legal document that apply to organisations who either release assets or those who collect them as part of an end of life asset disposal process. Where possible the requirement has been written verbatim but due to space some have been summarised, but the reference point will enable review against the original document.

REFERENCE POINT 81

When using a data processor, the data controller should only use processors who do the following:

REQUIREMENT	HOW ADISA CERTIFICATION MEETS THIS
Provide sufficient guarantees, in terms of expert knowledge and ability to deliver the service.	The ADISA Auditing process not only confirms verification that the service provider meets the industry-leading Standard in this area, but also includes a schedule of unannounced spot check audits. This measures continual conformance to the Standard AND via the FREE monitoring service enables data controllers to receive copies of audit documents in a timely fashion. The new ADISA Academy also provides members with a clear training path for their technical and operational staff to ensure they are constantly updated with required knowledge in order to perform their tasks.
Adhere to an approved code of conduct.	In July 2016 a code of conduct was approved by ADISA members with a view to it coming into use in January 2017.
Adhere to an approved certification mechanism.	The ADISA certification scheme is an established process and the auditing programme is currently working towards UKAS accreditation (ISO 17065) with the intention of achieving this in January 2017
Operate under the terms of a contract.	Within the ADISA Standard members have to have contracts in place with their customer OR be able to show where their customers refuse and therefore where the member identifies themselves as not accepting data processing responsibilities. ADISA is permitting a two year roadmap for this as it was only introduced in December 2015.

REFERENCE POINT 83

REQUIREMENT	HOW ADISA CERTIFICATION MEETS THIS
The controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks.	The ADISA Standard, written in 2010 and recognised by DIPCOG, is a risk assessment of the entire process. The audit summary reports (ASR) which are produced, highlight where risk to the integrity of the process exists and how each member has managed to mitigate that risk to an acceptable level. These documents are available to members' customers to help them meet this requirement.

REFERENCE POINT 84

REQUIREMENT	HOW TO COMPLY
The controller should be responsible for carrying out a data protection impact assessment for data processing operations.	Further to point 83, the ASR documents can be used by data controllers as the basis for, or as the document in entirety, for a data protection impact assessment.

ARTICLE 28 – PROCESSOR

REQUIREMENT	HOW ADISA CERTIFICATION MEETS THIS
The controller shall use only processors who provide sufficient guarantees to implement appropriate technical and organisational measures.	The ADISA Auditing process not only confirms verification that the service provider meets the industry-leading Standard in this area, but also includes a schedule of unannounced spot check audits. This measures continual conformance to the Standard AND via the FREE monitoring service enables data controllers to receive copies of audit documents in a timely fashion. The new ADISA Academy also provides members with a clear training path for their technical and operational staff to ensure they are constantly updated with required knowledge in order to perform their tasks.
The processor shall not engage another processor without prior specific or general written authorisation of the controller.	Within the ADISA Standard the use of downstream data processors is not permitted unless prior screening has taken place by ADISA or in a formal way by the member AND the data controller has authorised this.
The processor shall be governed by a contract.	Criteria 3.1 (a) and (b) within the ADISA Standard covers this.

REQUIREMENT	HOW ADISA CERTIFICATION MEETS THIS
Makes available to the controller all necessary information to demonstrate compliance with obligations laid out in their article and to allow for and contribute to audits, including inspections.	The ADISA Certification scheme is underpinned with an extensive audit process resulting in documented evidence pertaining to the delivery of the data processing service.
The processor shall immediately inform the controller if an instruction infringes this Regulation.	Criteria 3.1(b) requires ADISA members to inform their customers when despite requesting one, they cannot operate under a contract. Criteria 3.1(a) outlines critical elements to be included in the contract to enable the data controller to meet their regulator requirement.

ARTICLE 32 – SECURITY OF PROCESSING

REQUIREMENT	HOW ADISA CERTIFICATION MEETS THIS
The controller and processor shall implement appropriate technical and organisational measures to ensure a level of security to include a processor for regularly testing, assessing and evaluating the effectiveness of those measures to ensure the security of processing.	The ADISA Auditing process not only confirms verification that the service provider meets the industry-leading Standard in this area, but also includes a schedule of unannounced spot check audits. This measures continual conformance to the Standard AND via the FREE monitoring service enables data controllers to receive copies of audit documents in a timely fashion.

ARTICLE 33 – NOTIFICATION

REQUIREMENT	HOW ADISA CERTIFICATION MEETS THIS
The processor shall notify the controller without undue delay after becoming aware of a personal data breach.	As ADISA members do not know what data they are processing, the intention is to treat the loss of control over an asset that could carry data as being a data breach. In early 2017 ADISA will be launching an Incident Management Service for our members. This will include a notification process for their customers.
The controller shall notify the supervisory authority within 72 hours of becoming aware of it.	The Incident Management Service will also be available for Data Controllers to subscribe to and it will include a supervisory authority notification process.
The notification should include as much information regarding the incident as possible including measures taken or proposed to mitigate its possible adverse effects.	The Incident Management Service includes a structured review process including practical onsite interviews, forensics if required and a root cause analysis.

ARTICLE 35 – DATA PROTECTION IMPACT ASSESSMENT

REQUIREMENT	HOW ADISA CERTIFICATION MEETS THIS
The controller prior to processing shall carry out a data protection impact assessment for processing likely to result in high risk.	The ADISA ASRs can be used by Data Controllers as a means of pre-screening potential partners as they identify where risk exists and what countermeasures are in place to decrease that risk
The assessment shall include measures to evaluate risk and what mechanisms have been put in place to mitigate that risk.	

ARTICLE 40 – CODE OF CONDUCT

REQUIREMENT	HOW ADISA CERTIFICATION MEETS THIS
Associations and other bodies representing categories of processors may prepare a code of conduct and submit it to the supervisory authority for approval.	In July 2016 a code of conduct was approved by ADISA members with a view to it coming into use in January 2017.

ARTICLE 42 & 43 – CERTIFICATION AND CERTIFICATION BODIES

REQUIREMENT	HOW ADISA CERTIFICATION MEETS THIS
Certification shall be voluntary and via a process which is transparent.	The ADISA published Standard includes in great detail the certification process.
Processors which submit its processing certification shall provide the certification body with all information and access to conduct the certification process.	Within the new code of conduct this will be a requirement, as currently some information provided is not done so to a satisfactory level.
Certification bodies shall be accredited to ISO 17065.	ADISA does not currently hold this but is working towards achieving this and will do so in Jan 2017.
Certification bodies shall be able to demonstrate their independence and expertise in relation to the subject matter.	As a result of this requirement and also general dissatisfaction with its operation the ADISA Advisory Council is going to change with the council being operated outside of ADISA. (If it wishes to continue).
Certification bodies will have established procedures for the issuing, periodic review and withdrawal of data protection certifications.	The ADISA Audit Scheduling, Audit Review and Audit Failure processes meet this.
Certification bodies shall have established procedures to handle compliance and infringements of the certification or the manner in which the processor is operating under certification.	As part of the Incident Management Service any complaint or disclosure made to ADISA about a member by a third party would be classed as an incident and investigated. This will also be covered within the Code of Conduct.

CONCLUSION

It is widely acknowledged that the current procurement process for ICT asset recovery services is skewed heavily in terms of "price" and many in the industry who provide data processor services bemoan how data controllers currently approach this business process.

ADISA research can show evidence that more than 66 per cent of the UK public sector (on a sample size of over 400 respondents) currently break UK Data Protection law when disposing of ICT assets. As such, despite the EU Data Protection Regulation 2016 being very clear, not only in the few criteria identified above but throughout the entire document, that data controllers have much to do in order to comply with this legislation when disposing of assets, there will be some who will say: "so what, we have another law for organisations to ignore."

This fatalistic stance is understandable but it is clear when reviewing the reception to this new law that it is viewed as a sea-change in terms of regulation of the data protection efforts of organisations. Not only have the maximum fines (Article 83) increased to €20,000,000 or up to four per cent of global turnover there is also a requirement for mandatory breach notification (Article 33) within 72 hours. Mandatory notification is something already in place in many US states so let us view the EU GDPR definition of data breach: 'Personal Data Breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthourised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

ADISA's position is that, unless a data controller is able to demonstrate that they have engaged with data processing in such a way as to be viewed as complying with the EU GDPR, then the transaction would be viewed as unlawful, and therefore should be classed as breach.

At ADISA, we estimate that about 85 per cent of all collections made would currently fall into this category due to the lack of a contract, lack of a code of conduct and certification and lack of formal risk assessments being made. So does the future of asset disposal contain the majority of collections to be classed as data breach and requiring either party to disclose to the relevant data regulator? It certainly looks that way.

The good news for organisations is that our industry, operating as the final part of the data protection process, has been slowly getting our act together.

ADISA-certified companies operate to a rigorous published Standard and, more to the point, undergo continuous auditing to ensure compliance. The Standard was revised in December 2015 in preparation for the new EU GDPR and throughout the implementation of this law across Europe, ADISA and our members will be working hard to ensure that this is one group which operates to the law and helps their customers comply with law. Since January 2016 ADISA has suspended four companies and permanently excluded one. It makes sense for data controllers that, when looking to dispose of ICT assets, they should seek to engage with one of the ADISA-certified organisations. Not only will they be able to evidence compliance to the relevant parts of the new EU Data Protection Regulation 2016, but they will also know they are dealing with industry leading companies to whom they can entrust their brand, reputation and liability without undue concern.

WELCOME TO THE ADISA TRAINING ACADEMY

With content written by leading global experts in their field, ADISA is delighted to launch the first online training platform dedicated to ICT Asset Retirement and Disposal.

This on-line training platform provides content for any individual or organisation with an interest or responsibility for asset retirement and data protection. Its objective is to cater for both those releasing the assets and the industry providing asset recovery services.

WHAT IS COVERED WITHIN THE ACADEMY?

- Introduction to all aspects of IT Asset Disposal
- Identify security vulnerabilities which could occur within disposal
- Technical Considerations of how data is stored and sanitised on every media type
- How to write a risk based policy incorporating all aspects of disposal scenarios including encryption, cloud, BYOD etc.
- Key Stages in Policy Development
- How to build the value proposition when selling ITAD services
- Understanding the chain of custody and general asset management
- How to select and manage a vendor
- Identification of regulatory compliance requirements and how to meet them when disposing of assets

WHAT WILL GRADUATES BE ABLE TO DO?

- Understand risk within IT asset disposal
- Understand technical challenges within IT asset disposal
- Address and overcome security concerns
- Write and implement an asset disposal policy that mitigates risk of data loss and promotes re-use wherever possible
- Understand the IT disposal industry and how best to engage with it
- Achieve the maximum value return to the business
- Become subject matter experts within their organisation on legislation and standards which impact on IT asset disposal

ENROLMENT TO THE ACADEMY IS FREE AND ADISA MEMBERS GET ACCESS TO FREE COURSES. EACH COURSE COSTS BETWEEN £50/$75 AND £75/$110 WITH LEARNING PACKAGES AVAILABLE.

PLEASE GO TO **ADISA.GLOBAL** TO LEARN MORE

TONY BENHAM

THE GOOD, THE BAD AND THE UGLY – A TALE OF LIFE ON THE AUDIT TRAIL

I've been ADISA's lead auditor since October 2014 and performed nearly 150 audits in 10 countries. More than 66 per cent of them were unannounced - so I've seen pretty much everything this sector can offer. Or, in the words of one of my favourite films: the good, the bad and the ugly of what this sector can offer

As I approach my second year, this article is designed to give an insight into how our audit system works so companies can understand what we expect of them, and perhaps more importantly, how their customers can see the value of being the subject of such audits.

The examples below are real, although they never came from a single member. They are the accumulation of observations from various audits.

THE GOOD AUDIT

These begin in the knowledge that our admin team has completed all the pre-audit work. For example, prospective members have to complete a GAP analysis which will have been reviewed and have involved an on-site assessment. From here, remedial actions will have been recommended before audit day. When the member indicates they are ready, the full audit is scheduled and this the first time I get to see them. The information captured on the GAP analysis will have been transferred to the audit document and forms the basis of my assessment on the day.

For full audits involving existing members, the information captured during previous audits is consolidated and put into a document by the review team. This is then sent to the member for review, annotation or correction to ensure it forms an accurate description of their current activities.

For full audits I try to limit the time on site to a single day so I arrive bright

and early. I am usually greeted by a designated contact who will accompany me throughout my stay. After outlining the expectations from each party, I start with a tour of the building and warehouse, getting a feel for the place and taking any photographs I need.

I also collect samples of assets/consignments which will then become the reference points for the evidence needed for the report. Then we generally settle down in a room, often with others involved in the organisation's audit process, and work our way through the audit document.

Requests for documents can tend to slow things down and it's no surprise that one characteristic of an excellent audit is the ability of the designated person(s) to have ready access to the evidence I've requested; be it sending documents via email or scanning and emailing hard copies.

I can really tell the difference between a well-prepared and motivated member as opposed to one who needs me to explain criteria or, in some cases, challenging the need for criteria to even be in the published Standard.

In short, the secret to a good audit is easy: thorough preparation and provision of appropriate evidence for each criterion by the ITAD - after all, we only measure you against things you say you do.

Strong motivation by the company, and especially my designated individual(s), to, not only pass the audit, but to do so with a high score is also key.

As ADISA has grown we have met, peculiar as it seems, some resistance on audit day. We suspect that this is either due to the Standard being forced upon the operational team or that the company as a whole isn't motivated to embrace the justification for the Standard.

> **COMPANIES WHO ARE WELL PREPARED GENERALLY FLOW THROUGH THE FULL AUDITS WITHOUT TOO MANY ISSUES**

These types of audits are few and far between as the pre-audit process generally weeds these types of prospective members out. One thing is consistent though; companies who are well prepared generally flow through the full audits without too many issues and go on to become members of excellent standard.

Unannounced audits are more challenging as members have no time to prepare. Generally, good unannounced audits are where my arrival is greeted with openness, transparency and support from staff well-prepared to provide the requested evidence. It's, therefore, more the attitude than the results that classifies an unannounced audit as good.

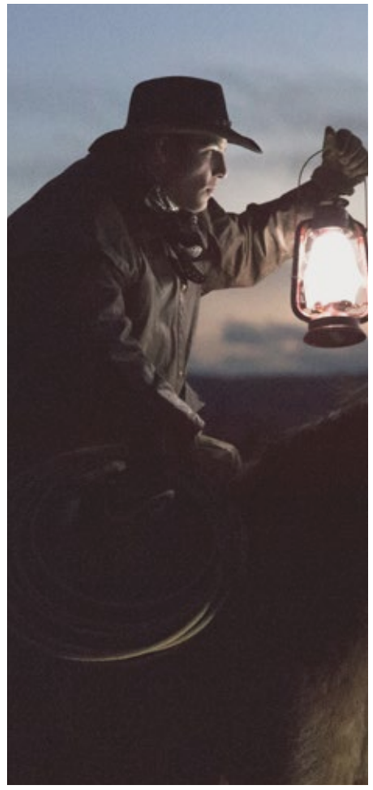
At ADISA we know businesses have limited resources and that it can be a drain to draw on them at these audits. But those who embrace this as a key way of showing to their customers that they do protect their data, present themselves professionally and without grumble. So even though there may well be remedial action required - and in some cases urgent action - a good unannounced audit is always about attitude and, where action is required, some members do it on the spot, making my life much easier.

Of course at unannounced audits we do our forensic testing and here is where members do get nervous. As ADISA states, we HAVE found data and have always investigated and resolved issues.

As such, when I select my sample of devices to be tested and sit down to begin, it must be like waiting for exam results - too late to do anything about it, but nerve-wracking nonetheless.

Of course, mistakes happen but it is how we address them that is key. I've found data due to badly configured software (In the hidden partitions, not on the user areas), due to human error and a process failure.

In all of these, the root causes were identified quickly, and in the case of one member, action was taken before I even left site! Their recovery was so swift and decisive that what potentially began as a



very bad audit became what I would call a very good and successful one, both from their perspective and ours.

ADISA members take such issues extremely seriously and to actually have one thank us for identifying these issues shows that it's not all about catching people out but protecting them and their customers.

THE BAD AUDIT

So what makes a bad audit? As mentioned above, it's not so much the results but the attitude of the member. For full audits, the member, prospective member, or specific members of staff can often display a profound lack of understanding of the ADISA Standard and the evidence required for the criteria.

A realisation dawns on us early on that things aren't going to go well when some of our basic requirements are met with blank stares. Of course, everyone deserves a bad day, but we have had situations where even our pre-audit process has been ignored.

The attitude to certification in some companies needs addressing. I've had situations where staff look at me to provide them with the answers. My job is not to help them pass, but to evidence that they meet the criteria which enables them to pass. I'm not sure how other audit processes go but ours isn't about coaching members to meet our requirements.

There are other aspects of a bad audit such as unprofessional behaviour; designated staff talking on their phones, between themselves or sending messages rather than providing me with evidence.

We have even had a member move premises and begin to operate from a different warehouse and building without informing and involving ADISA

> **WHEN I SELECT MY SAMPLE OF DEVICES TO BE TESTED AND SIT DOWN TO BEGIN, IT MUST BE LIKE WAITING FOR EXAM RESULTS**

first. What's more, the owner/manager didn't think they had done anything wrong!

Another member provided such a poor response to audit that they argued about their failure for three months. Needless to say, neither of these companies are ADISA members any longer.

THE UGLY AUDIT

Whilst many would say that, surely, the worst audits are the bad ones, from my perspective there is another category – the ones which are just plain difficult to complete and generally take the most time.

These can be where a prospective member has introduced new processes to meet our requirements and their sales and operations teams are still bedding them in. When I look to capture evidence of compliance in these situations there can be indecision, even fear, because the processes are new, and in some cases, not yet being adhered to.

Even in some existing members, where ADISA certification doesn't come as second nature, there have been audits where I've seen a clear slippage from where the company was on the previous visit.

> SOME EMBRACE CERTIFICATION AS A WAY OF IMPROVING OPERATIONS SO THEIR CUSTOMERS RECEIVE A CONSISTENT SERVICE

These are both ugly audits as there is simply not the evidence across all samples taken to show compliance and so remedial actions are required. For some, these prove too much and they leave the program but others who embrace certification, view this as a way of improving operations so that their customers receive a secure consistent service all the time.

Another example is when I arrive at the premises at the agreed time only to find that that the designated people are not there yet or they are still gathering paperwork and not ready to start.

This manifests itself in the member not being able to provide the evidence on audit day and/or not sticking to deadlines for the post-audit evidence requirement. Some basic things, such as not being given a suitable place to work, or the designated person being badly prepared and having to leave at regular intervals to ask management for advice or to seek evidence from somewhere in the business. Ugly audits are just pure hard work for all involved but do not happen often and are generally one-offs as we either work through such issues or the member leaves the programme.

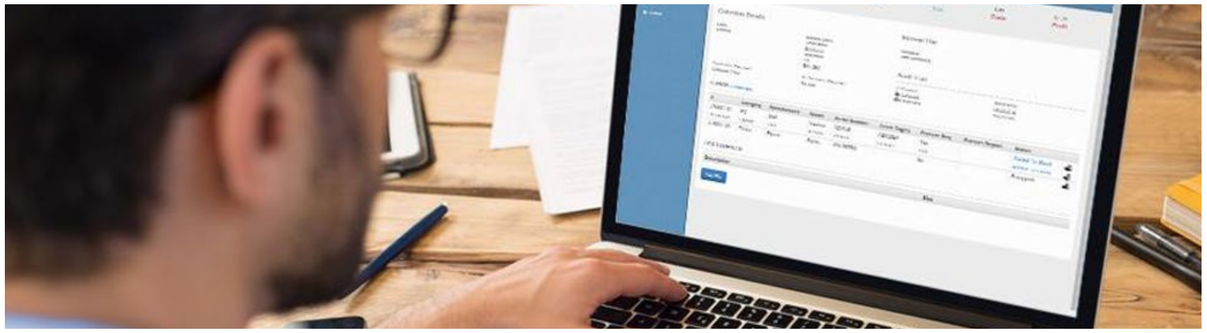
As the ADISA programme matures, my own experience improves and the members' understanding of the process improves, the number of audits classed as good is by far in the majority. However, when an audit turns bad it generally is very bad, and when they go ugly . . . well the least is best said about them!

Whatever category an audit falls into, it is the overall audit history which is best reviewed to see the evolution of an ADISA member. Our audit summary reports show how members perform across all audits and, we feel, show how members in good standing achieve the high quality results, as you would expect.

For my part, it's been a significant learning experience coming from an academic background but I can honestly say that it's been a steep but enjoyable learning curve and I look forward to pushing this audit programme onwards.

ITADCOLLECT: A CLOUD-BASED COLLECTION MANAGEMENT SOFTWARE SOLUTION

It's essential that any ITAD has a proper system in place to provide full traceability of all items being handled. While there are a few options on the market, most solutions have a hefty price tag, putting them out of reach for start-up companies. That's why we decided to create ITADCollect



Last year we entered talks with a UK-based ITAD to discuss creating a new product, specifically designed with the small ITAD in mind. We wanted something that offered a cost-effective solution for start-ups, but had the flexibility to grow and adapt to much larger organisations. After a few months' development, ITADCollect was born, and our initial customer was switched over to the platform.

Designed as a cloud-based solution, ITADCollect is accessed through the web browser, making it compatible with all devices, from PCs to Macs, and mobile devices such as iPads, tablets and smart phones. As long as you have a web connection, you can access your data and work the way you want, from the devices that best meet your needs.

> ITADCOLLECT HAS TRANSFORMED OUR BUSINESS. WITHOUT IT WE JUST COULDN'T PROVIDE THE TRACEABILITY THAT MANY OF OUR CUSTOMERS REQUIRE. REDUCING PAPERWORK, AND PROVIDING EVERYTHING WITHIN ONE SYSTEM HAS BEEN A GREAT BENEFIT TO US
>
> DENVER, GIGACYCLE

Mobile compatibility is at the heart of ITADCollect, allowing your employees to use the system directly from a customer's site while a collection is taking place. This creates a far quicker feedback loop – no longer do you need to wait until the collection is processed in your office – you can see changes in real time as it is collected.

But just tracking your collections isn't enough. While most software solutions only cover the collection stage, ITADCollect also has a full stock tracking and sales management facility.

By tracking the full life-cycle, we can provide traceability from start to finish, from collection, through processing, to re-sale.

Everything in ITADCollect is tied together. As soon as a collection is processed, the item becomes available for sale, and will show up in your stock list. Once it is sold, the sale is recorded in the system, and tied back to the original collection. With a couple of clicks you can see where a particular stock item was collected from, what happened to every item from a collection, and how much the resale value was for this collection.

ITADCollect has now been released on the market. Request a demo now and find out how we can help your business.
www.itadcollect.com

JEFFREY DEAN

THE DATA SECURITY ACT OF 2015 NATIONAL DATA SECURITY BREACH AND NOTIFICATION STANDARDS

Jeffrey Dean worked in US military counter intelligence before taking security roles at leading corporations. Here, Jeff takes a look at the regulatory landscape where data protection is concerned

INTRODUCTION

Despite the alarming rise in the number of data breaches and the increasing sophistication of cyber-threats, a single federal standard to protect financial account and non-public personal information currently does not exist. With recent data security breaches having put millions of confidential records at risk, the need to pass legislation to establish such a standard could not be more evident.

CURRENT LEGISLATION

General Laws

Information security laws are designed to protect financial account and sensitive personal information from compromise and unauthorised disclosure, acquisition, access, or other situations where unauthorised individuals have access or potential access to that information for unauthorised purposes. No single federal law or regulation governs the security of all types of sensitive personal information. Instead, the US has a patchwork system of federal and state laws, and regulations that can sometimes overlap, dovetail and contradict one another. In addition, there are many guidelines, developed by government agencies and industry groups that do not have the force of law, but are part of self-regulatory guidelines and frameworks considered "best practices".

These self-regulatory frameworks have accountability and enforcement components that are increasingly being used as a tool for enforcement

by regulators such as the Federal Trade Commission (FTC). The proliferation of security breaches has led to an expansion of this patchwork system of privacy laws, regulations and guidelines which is becoming one of the fastest growing areas of legal regulation.

The combination of an increase in interstate and cross-border data flow, together with the increased enactment of data protection-related statutes heightens the risk of privacy violations and creates a significant challenge for a data controller to negotiate the onerous and often inconsistent requirements for each State.

Sectoral Laws

There are many federal privacy-related laws that regulate the collection and use of personal data. Some apply to particular categories of information, such as financial or health or electronic communications. Others apply to activities that use personal information, such as telemarketing and commercial e-mail. There are also broad consumer protection laws that are not privacy laws per se, but have been used to prohibit unfair or deceptive practices involving the disclosure of, and security procedures for protecting, personal information.

Some of the most prominent federal privacy laws include, without limitation:

- The Federal Trade Commission Act (15 U.S.C. §§41-58) (FTC Act) is a federal consumer protection law that prohibits unfair or deceptive practices and has been applied to off and online privacy and data security policies.

- The Financial Services Modernisation Act (Gramm-Leach-Bliley Act (GLB)) (15 U.S.C. §§6801-6827) regulates the collection, use and disclosure of financial information. It can apply broadly to institutions such as banks, securities firms and insurance companies, and other businesses that provide financial services and products.

- The Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. §1301 et seq.) regulates medical information. It can apply broadly to healthcare providers, data processors, pharmacies and other entities that come into contact with medical information.

- The HIPAA Omnibus Rule also revised the Security Breach Notification Rule (45 C.F.R. Part 164) which requires covered entities to provide notice of a breach of protected health information. Under the revised rule, a covered entity must provide notice of acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule, unless the covered entity or business associate is able to demonstrate that there is a low probability that the protected health information has been compromised.

- The Fair Credit Reporting Act (15 U.S.C. §1681) (and the Fair and Accurate Credit Transactions Act (Pub. L. No. 108-159) which amended the Fair Credit Reporting Act) applies to consumer reporting agencies, those who use consumer reports (such as lenders) and who provide consumer reporting information (such as credit card firms).

- The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) (15 U.S.C. §§7701-7713 and 18 U.S.C. §1037) and the Telephone Consumer Protection Act (47 U.S.C. §227 et seq.) regulate the collection and use of e-mail addresses and telephone numbers, respectively.

- The Electronic Communications Privacy Act (18 U.S.C. §2510) and the Computer Fraud and Abuse Act (18 U.S.C. §1030) regulate the interception of electronic communications and computer tampering, respectively.

State Privacy Laws

There are many laws at state level that regulate the collection and use of personal data. And the number grows each year. Some federal privacy laws pre-empt state privacy laws on the same topic.

As of June 2016, 47 states, as well as the District of Columbia, Puerto Rico and the US Virgin Islands all have enacted laws requiring notification of security breaches involving personal information. At least 31 states have enacted laws that require entities to destroy, dispose, or otherwise make personal information unreadable or undecipherable.

And at least 12 states – Arkansas, California, Connecticut, Florida, Indiana, Maryland, Massachusetts, Nevada, Oregon, Rhode Island, Texas and Utah—have imposed broader data security requirements. Some states, such as California and Indiana, impose the general requirement that organisations implement and maintain reasonable safeguards to protect personal information from unauthorised disclosure or use.

Nevada and Massachusetts impose more granular requirements. Nevada requires organisations that collect payment data to comply with the PCI Data Security Standard. Massachusetts insists organisations maintain written data security programs that include requirements such as oversight of third-party service providers, risk assessments and imposing for violations of security policies.

DATA SECURITY ACT OF 2015

In May 2015, Reps. Randy Neugebauer, R-Texas, and John Carney, D-Del. introduced a bipartisan bill, the Data Security Act of 2015 (H.R. 2205), setting data protection standards, outlining a process for notifications and recognising financial institutions' compliance with the Gramm-Leach-Bliley Act. (https://www.congress.gov/bill/114th-congress/house-bill/2205/text) This House bill comes several weeks after a Senate bill (S.961) was introduced by Sens. Tom Carper (D-Del.) and Roy Blunt (R-Mo.) that would set standards for entities that handle consumers' personal information. The purposes of the House bill are:

1. To establish strong and uniform national data security and breach notification standards for electronic data; and

2. To expressly pre-empt any related State laws in order to provide the Federal Trade Commission with authority to enforce such standards for entities covered under the Act.

H.R. 2205 requires individuals, corporations, or other non-government entities that access, maintain, communicate, or handle sensitive financial account or non-public personal information to implement an information security program and to notify consumers, federal law enforcement, appropriate administrative agencies, payment card networks, and consumer reporting agencies of certain data breaches of unencrypted sensitive information likely to cause identity theft or fraudulent transactions on consumer financial accounts. The act further requires individuals, corporations, or other non-government entities to:

1. Develop and maintain an effective information security program tailored to the complexity and scope of its operations, and the sensitivity of its data;

2. Oversee service providers with access to customer information, including requiring service providers by contract to take appropriate steps to protect the security and confidentiality of this information;
3. Train staff to prepare and implement its information security program;
4. Test key controls, systems and procedures of its information security program;
5. Adjust its information security program to reflect the results of its ongoing risk assessment;
6. Provide special notification procedures for: (1) third-party service providers that maintain data in electronic form on behalf of another entity (Third-Party Service Provider is defined as any person that maintains, processes, or otherwise is permitted access to sensitive financial account information or sensitive personal information in connection with providing services to a covered entity);
7. Allow financial institutions to communicate with account holders regarding breaches at third-party entities with access to their account information; and
8. Set forth alternative compliance procedures for: (1) financial institutions and affiliates under the Gramm-Leach-Bliley Act, and (2) entities complying with certain health record privacy laws.

Each covered entity shall develop, implement, and maintain a comprehensive information security program that contains administrative, technical and physical safeguards that are reasonably designed to:

1. Ensure the security and confidentiality of sensitive financial account information and sensitive personal information;
2. Protect against any anticipated threats or hazards to the security or integrity of such information; and
3. Protect against unauthorised acquisition of such information that could result in substantial harm to the individual to whom such information relates.

Breach of Data Security

Under this Act, the term "breach of data security" means the unauthorised acquisition of sensitive financial account information or sensitive personal information. It does not include the unauthorised acquisition of sensitive financial account information or sensitive personal information that is encrypted, redacted, or otherwise protected by another method that renders the information unreadable and unusable if the encryption, redaction, or protection process or key is not also acquired without authorisation.

If a covered entity believes that a breach of data security has, or may have, occurred, the covered entity shall conduct an investigation to:

1. Assess the nature and scope of the incident;
2. Identify any sensitive financial account information or sensitive personal information that may have been involved in the incident;
3. Determine if the sensitive financial account information or sensitive personal information has been acquired without authorization; and
4. Take reasonable measures to restore the security and confidentiality of the systems compromised by the breach.

If a covered entity determines that the unauthorised acquisition of sensitive financial account information or sensitive personal information involved in a breach of security is reasonably likely to cause substantial harm to the consumers to whom the information relates, the covered entity, or a third party acting on behalf of the covered entity, shall make notification, without unreasonable delay to:

1. An appropriate Federal law enforcement agency;
2. The appropriate agency or authority;
3. Any relevant payment card network, if the breach involves a breach of payment card numbers;
4. Each consumer reporting agency that compiles and maintains les on a nationwide basis; and
5. All consumers to whom the information relates.

In addition, in the event of a breach of security of a system maintained by a third-party service provider that has been contracted to maintain, store, or process data in electronic form containing sensitive account information or sensitive personal information on behalf of a covered entity which owns or possesses such data, such third-party service provide shall:

1. Notify the covered entity; and
2. Notify consumers if it is agreed in writing that the third-party service provider will provide such notification on behalf of the covered entity.

On December 9, 2015, the House Financial Services Committee approved H.R. 2205 in a 46-9 vote. The legislation now awaits further action before the full House of Representatives.

References

(2015) H.R.2205 – Data Security Act of 2015; Congress.gov

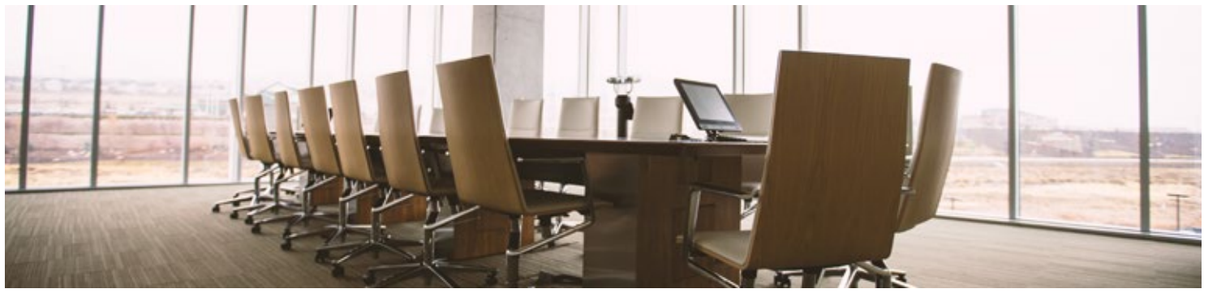
(2015) Data protection in United States: overview. Practical Law; A Thompson Reuters Legal Solution

(2014) Outlook for State Data Security Laws: More than Breach Notification; IAPP.ORG

GILL BARSTOW, ORBIT

WHY ACCOUNT PLANNING IN ASSET DISPOSAL?

The sales process can be complex, the decision-making process may not be immediately clear, and you may need to educate the customer to understand the value. So the right account strategy is vital



Most B2B companies get 80 per cent of their income from the top 20 per cent of their accounts. Below those major accounts is usually a layer of potential 'rising stars' – accounts which need a well thought-through strategy, some research, planning and a little more TLC. With that, many of these silver level accounts could become gold level and generate significant incremental income.

It costs six times more to sell to a new customer than it does to sell to an existing one. Most companies have enough potential in their current account base to achieve growth plans without needing to forge "net new" relationships. In a challenging market this is an area of "lower hanging fruit" that cannot be ignored. Account planning has long been accepted as an important tool in developing major accounts. However, many organisations struggle with making it stick. A lot of effort is put into getting it going, only for it to be abandoned. Sales people view it as an onerous, administrative, over-complex process.

Account planning only brings benefits if your sales team do it consistently. However, there are remarkable benefits in doing this well – so what benefits would you like to gain from **account planning?**

Widening your footprint and breaking through into new areas of the client company, leading to **increasing your opportunities to sell**	**Moving up the value chain and building relationships at more senior levels** leading to an **increased influence over the solution and the decision making process.**	**Selling the full range of your offerings** as solutions rather than individual products or services and leading to **increasing share of wallet**
Presenting products and services in a compelling way, linked to client's business issues leading to **helping clients see the return on investment from your solutions**	Positioning your company as a **strategic supplier,** and yourself as a **trusted advisor,** leading to increasing client loyalty and **differentiating you from your competition**	**Increasing the margin from your major accounts** through **increasing the % of higher value services** and also **reducing price sensitivity** and **building a stronger annuity stream**

Do these benefits sound attractive? What impact would it have in your sales operation if more of your sales people could work in this way?

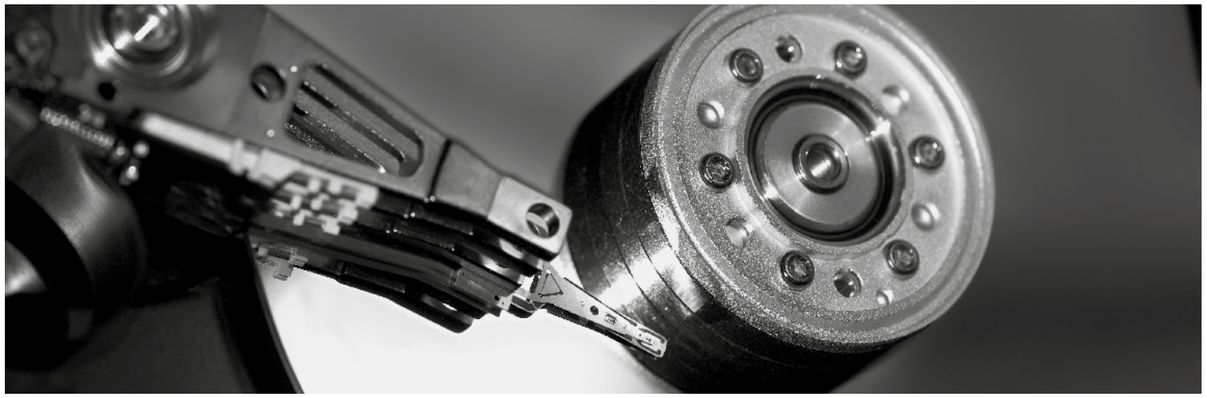
Orbit Business Development are a business and people change consultancy with a strong track record in the IT mid-market. **Click here** to download their FREE white paper on 'Making Account Planning Stick'

ANTONY BENHAM, UNIVERSITY OF SOUTH WALES

EXPLORING THE HIDDEN AREAS ON ERASED DRIVES

When can an erased magnetic hard drive be classed as data-safe may seem a moronic question. After all, once all the data is erased surely it's safe? To answer this question you have to understand more about magnetic hard drives themselves and then consider the concept of threat and threat capability.

This article is a heavily edited summary of a white paper written by ADISA's own Anthony Benham and Gareth Davies of the University of South Wales. It is recommended to read that in full as it is comprehensive and technical.



UNDERSTANDING HARD DISK DRIVES

Logical layout of a magnetic hard disk drive.

When a hard drive is manufactured, it comprises various sections designed to increase the reliability, performance, security and safety of the device.

These sections include the User Accessible Area (UAA), Host Protected Area (HPA), Device Configuration Overlay (DCO), Service Area (SA) and Reserved Area (RA) shown in figure 1.

At this point it's important to begin to consider how these different areas are accessed as that is crucially important when considering secure sanitisation.

Typically speaking, the UAA is accessible by the user of the device and it is here that files are typically stored during normal drive operations.

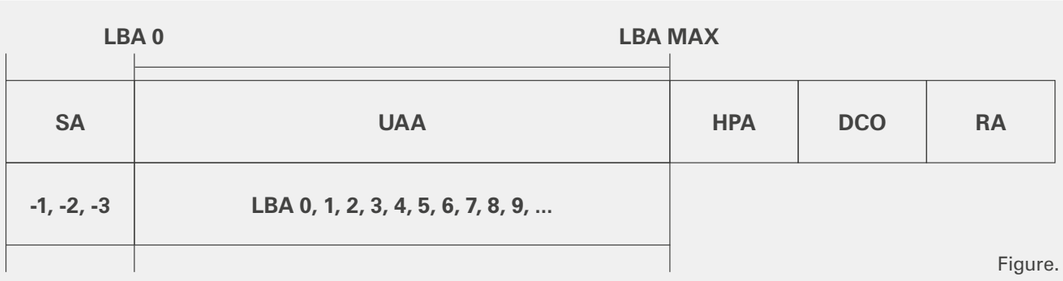


Figure. 1

USER ACCESSIBLE AREA (UAA)

The user accessible area - or the user area - is the section of a hard disk that holds the operating system being used and all the user files.

The user area can have multiple partitions that can include multiple operating systems, ie: two partitions, one with windows and another with Linux.

Although it can be thought that the partitions are completely separate, because they are in the user-accessible area of the hard disk, regardless of how many partitions there are, a standard forensic tool such as FTK will be able to successfully obtain all partitions when creating an image.

It is standard practice for a forensic investigator to create a bit-for-bit copy of an entire hard drive. This is how a forensic image is created.

However, this statement only covers the 'user accessible area' of a hard drive, and does not apply to the "entire hard drive".

The user area is completely isolated from other areas of the hard disk. This protects the other areas from corruption or damage through being accessed by a user, either accidentally or deliberately.

The service area (SA) requires commands that have been specifically created by the hard drive vendor to access. These areas are completely isolated from the operating system and are not accessible by the OS or user.

HOST-PROTECTED AREA (HPA)

The Host Protected Area or HPA was introduced with the ATA-4 standard [3] and was designed as a hidden area to store information that cannot be easily accessed, modified or changed by a user, BIOS or operating system, [8]. The motivation behind the introduction of the HPA was to implement a location where the manufacturers could safely store data that would not be removed when a user formats or erases the data on the hard drive.

Many hard disks have a HPA size of 0 by default however, by utilising these commands a HPA can be created with ease. An example of this is displayed below, where the command SET_MAX_ADDRESS is used to set the maximum numbers of sectors a user can access to less than the maximum addressable physical sectors on a hard disk, which can be found using READ_NATIVE_MAX_ADDRESS. Finally once complete, combining the IDENTIFY_DEVICE command with the READ_NATIVE_MAX_ADDRESS command will create and reveal the Host Protected Area.

DEVICE CONFIGURATION OVERLAY (DCO)

The Device Configuration Overlay was introduced with the ATA-6 standard [4]. It was implemented as manufacturers were creating hard drives that would differ slightly in capacity, i.e. 501GB, 509GB etc. In order to ensure the hard drives were maintaining a particular standard and size, the DCO hidden area is used to hide sectors from the User Accessible Area so that a consistent hard drive size is maintained [9]. The DCO can also be used to limit hard drive functions and parameters. As with the Host Protected Area, The Device Configuration Overlay area can be added to, modified and removed using standard ATA commands.

SECURITY RISKS POST DATA ERASURE

In order to measure risk posed by data in different parts of the magnetic hard drvie we must first have to look at what data could reside in these areas and then look at how user data might find its way into these areas. We can then review how data erasure techniques can be used to manage this risk.

DATA STORED IN HIDDEN AREAS OF A MAGNETIC HARD DRIVE

HOST PROTECTED AREA (HPA)

The Host Protected Area or HPA is an area on the drive that is not addressable by the OS or the BIOS. Here is stored the information for the recovery of hard drive during a repair mode. It contains the hard drive diagnostics and an image of the OS already on the drive. HPA is a known sophisticated malware or rootkit location, for malicious attackers to embed code, such as viruses and root kit. Its session volatile nature means its space can be easily written to or the HPA can be altered in such a way as to write code into the OS image within it.

The image stored in the HPA comes from the OEM but an admin can configure this HPA legitimately to a custom version, to contain more user information. For example, for a company network, the admin can configure this image to contain user data, such as network configurations and user logins to speed up deployment of network.

A company could conceivably redeploy an old or new resource with a resident infected HPA, from one department to another for example or it could sell it to another organization or individual. In doing so, the malware such as virus, worm or rootkit can spread to new host(s) and hence a new network. Living in the HPA space, a root kit can survive erasure, reformatting and virus scans.

It is also possible for a user to extend and manipulate the HPA of their own drive and hide their user data. The LBA Max address can be retracted accommodate new HPA space, using the SET_MAX_ADDRESS command,

in both volatile and non-volatile modes. In the latter, the drive will retain the new address even after power down. The data space provided for the HPA now has user data. HPA can be extended in size without overwriting the previously user data addresses it has gained. Therefore there is now user data that is not addressable by the OS and yet is present and accessible in the HPA space. See figure 3.

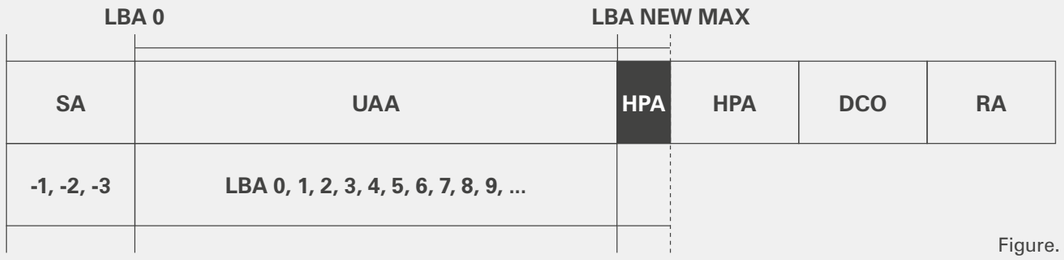


Figure. 3

DEVICE CONFIGURATION OVERLAY (DCO)

The Device Configuration Overlay is used by manufacturers to configure drive sizes. A malicious user can either manipulate a DCO to make it bigger to capture user data, as with HPA or a determined sophisticated attacker can inject data into the DCO space just as data can be injected into the firmware space. The DCO can then be removed allowing access to pervious user data or embedded code. This data or code will survive reformatting and virus detection and can also survive erasure. [10]

However, it is far more difficult to attempt to manipulate or inject data into the DCO as opposed to HPA, due to the non-volatile and permanent nature of its SET_MAX_ADDRESS command. The attack to manipulate it and/or inject it will have to be of IS5 C or D category. Not much work has been published officially in this area but experience working with HDD structure and firmware manipulation within the advanced data recovery field tells us that this is the case. [11]

Overwriting Standards

The main certification schemes / standards for overwriting tools are CESG (UK), Common Criteria and NIST 800-88 (US). Below is a very quick summary of their requirements.

CESG's CPA approval scheme (for overwriting products) has a published crtieria which software vendors must meet in order to achieve certification. This is called the Security Characteristcs and it is worth reviewing this to fully understand the benefit of using products which meet this criteria.

CONCLUSION

In conclusion, for any organisation looking to specify the type of overwriting to use on a magnetic hard drive they should first consider against whom they are protecting themselves. At that point they should look at options for specifying an overwriting standard and a product to be used. These two parts are essential because there are many products on the market claiming compliance with the overwriting standards but not holding any validation that they meet them. Furthermore, the vendors utilising the software must know how to configure it in order to ensure it is being used correctly. ADISA's position is that throwing HPA and DCO are two areas on a hard disk drive that are not accessible to the operating system or the BIOS and are outside the user addressable space. HPA has recovery data for the drive while the DCO is a disk size configuration utility. The HPA has been known to be used by malicious attackers to inject malware and root kits. The DCO can have the same issues but is much harder to achieve. For currently known attempts, a successful attack on the DCO of a hard drive needs to have laboratory IS5 category C or D attack, which is far more sophisticated in nature than an attack to attain the same results on the HPA space. It is essential that the HPA be removed on erasure of a drive.

ALAN DUKINFIELD, S2S

LET'S TAG, LET'S READ...

In conjunction with a leading University S2S has developed a closed-loop RFID system to track end-of-life IT and mobile phones from receipt, through the processing system to re-sale as a refurbished asset

As soon as a product arrives at S2S it is fitted with an RFID tag. A series of RFID readers located throughout the processing facility allow it to be tracked through a series of stages until product completion. The process provides 'live' information to users and customers through a database and web portal that display exactly where products are in the process.

The stages include asset-tracking of the unique product identifier, PAT testing, functional testing, data erasure and repair and can be adapted to suit specific user or client requirements. Product process maps for particular products set out process routes which must be followed from receipt to completion to ensure stages cannot be overlooked.

Furthermore, interfaces with leading data erasure packages have been developed so that 'data erasure reports' are automatically downloaded to the system's database and web portal, in real time for all data holding devices. This enables to the system to check the data status of the product before the process is completed, ensuring maximum data security for users and clients. The system also allows the operator to test products to PAS141 Standard if required by the client. Reports available from the system include asset manifests, stock lists, sold stock lists and repair reports along with a host of other management information including fault reports, process timings and 'live' job progress.

2016 will see the movement of the 'tagging' of assets from receipt at S2S's premises to tagging the product before it leaves the clients premises. This will ensure visibility of products during transportation and arrival at the processing site along with on and off-site electronic manifest sign-off and client email updates. This will give complete visibility of product from the client's premises through to either the recycling or resale of the product, depending on its condition.

ADISA CERTIFIED MEMBERS

UNITED KINGDOM AND REPUBLIC OF IRELAND
ADISA CERTIFIED ITAD MEMBERS

- Absolute IT Asset Disposals
- AMI Limited – Belfast
- AMI Limited – Dublin
- Arrow Value Recovery
- Asset Care
- Bell Intergration
- Blackmore Ricotech
- BTR UK Limited
- Centreprise
- Charterhouse Muller UK Limited
- Computer Disposals Limited
- Computer Recyclers
- EOL IT Services
- Gigacycle
- Future Generation Disposals
- Greensafe IT Limited
- ICEX Ltd
- ICT Reverse
- Insurgo Media Services
- IT Renew
- Lombard Technology Services
- MacColl Media
- Procurri UK LTD
- RDC
- RecycleIT
- Re-tek UK Ltd
- Reuse Technology Group
- S2S
- SCC
- Secure IT Disposals
- Sims Recycling Solutions – Dumfries
- Stone Group
- Technimove
- Tes-Amm- Irvine
- The ITAD Works
- Tier 1 Asset Management
- Ultratec

ADISA CERTIFIED LOGISTICS MEMBER

- Bishopsgate
- Bonds
- SAS Logistics

ADISA CERTIFIED SERVICE

- Joyce Solutions – Migration Services

REST OF EUROPE
ADISA CERTIFIED ITAD MEMBERS

- Alfanet S.A. – Greece
- Arrow Value Recovery (EMEA) Czech Republic
- Arrow Value Recovery (EMEA) Netherlands
- Arrow Value Recovery (EMEA) Belgium
- Arrow Value Recovery (EMEA) Germany
- Arrow Value Recovery (EMEA) France
- Diskshred (Mobile Destruction) Germany
- Sims Recycling Solutions – Germany
- Sims Recycling Solutions – The Netherlands
- Sims Recycling Solutions – Poland
- Sims Recycling Solutions – Czech Republic

CANADA
ADISA CERTIFIED ITAD MEMBERS

- ITRenew – Ontario, Canada

UNITED STATES
ADISA CERTIFIED ITAD MEMBERS

- Arrow Value Recovery – Reno, NV
- Arrow Value Recovery – Richmond, VA
- Arrow Value Recovery – Dallas, TX
- Arrow Value Recovery – Columbus, OH
- Arrow Value Recovery – Hartford, CT
- ITRenew – Newark, CA
- ITRenew – Austin, TX
- ITRenew – Las Vegas, NV
- ITRenew – Denver, CO
- ITRenew – Sterling, VA

REST OF THE WORLD
ADISA CERTIFIED ITAD MEMBERS

- Sims Recycling Solutions – Singapore
- Sims Recycling Solutions – India

SEARCH FOR A CERTIFIED COMPANY HERE:
ADISA.GLOBAL/SEARCH-FOR-A-CERTIFIED-COMPANY

ADISA NEWS

ASSETCARE GROWTH CONTINUES

In 2008 the WasteCare Group (AssetCare's parent company) established BatteryBack Plc, with the aim of being the UK's leading battery producer compliance scheme. Veolia were invited to become joint owners. Since the introduction of the regulations in January 2010, BatteryBack has been the largest of the six UK compliance schemes with over 55 per cent of the UK's obligation. On June 1, 2016, the WasteCare Group bought Veolia's shareholding in BatteryBack Plc. WasteCare is also the largest collector of portable batteries in the UK, with over 30,000 collection points, making it responsible for over 60 per cent collected.

Combine this with the UK's largest Battery Producer Compliance Scheme and it is clear that BatteryBack are best-placed to benefit from economies of scale and provide the lowest sustainable obligation costs in the UK, currently, a fraction of those in the rest of Europe.

To ensure Britain fulfils its recycling obligations for portable batteries in coming years, BatteryBack's plan is to increase the number of recycling points to over 100,000, focusing on schools, public buildings and the workplace. There are also plans to build Britain's first recovery plant capable of processing the country's entire alkaline and lithium battery output.

WasteCare will continue to have a strong relationship with Veolia. Given the challenges ahead, it was agreed that one owner would be more effective than two, although both companies may be involved with the battery recycling plant.

The news comes hot on the heels of WasteCare's April acquisition of Greif's steel packaging recycling operation in Avonmouth and AssetCare's purchase of the PHS Maxitech business last summer. The steel packaging operation will allow WasteCare's PackCare division to provide a true one-stop shop for all types of industrial packaging, regardless of volume, type and contamination.

NEW SERVICE FOR TAPE RE-USE

On April 18, Insurgo Media passed their initial audit against the published ADISA Asset Recovery Standard. They achieved an excellent score and reached 'Distinction' level. One element of this process which is different for Insurgo was that they offer a proprietary solution for magnetic tape re-use. This solution utilises their own

INSURGO Media

proprietary equipment, KIT (Kills Information on Tape). This hardware has been precision-engineered to 'Degauss' the Data Tracks on LTO and 3592 Media whilst shielding the Magnetic Servo tracks, and enabling the tape to be re-used. The solution has been designed to run the full length of the tape, ensuring complete Data Erasure. The Insurgo service includes bespoke software that lets them track each tape at serial number level, so full traceability is achieved.

To ascertain the effectiveness of the tape process additional testing was carried out, following this method:

1. LTO and 3592 tapes had control data written on them at the University of South Wales. These tapes were collected by an ADISA auditor and taken to Insurgo on audit day.
2. During the audit process the tapes were presented to Insurgo and auditor witnesses the application of the proprietary solution to sanitise the data.
3. The tapes were returned to the university for forensic assessment.

The result was that no data was recovered from the sample of LTO drives. For details of the forensic tests and the subsequent report please read Claims Test Report Insurgo June 2016 V1.3

The tests were led by Professor Andrew Blyth who described tape "as an interesting media as data is written on to it in a linear fashion, making recovery relatively easy when faced with any length of tape. For that reason the destruction of tape is typically done by shredding and there are specialists in this field who do a great job. However, we've seen some shredding done by shredders not intended for use with tape leaving lengths of tape still intact, making recovery simple. Of course, there are higher-end tape shredding solutions which are extremely effective as well as degaussing. But the Insurgo solution was the first time we've seen anything which permitted the re-use of tape without risk to the previous owner's data."

ADISA CEO Steve Mellings said: "We've been working with Insurgo for some time and I'm delighted that their work has now been taken to market. As part of their certification they will be undergoing our normal round of unannounced auditing but we will also repeat the tests done on their tapes. This is designed to give customers of Insurgo confidence that their tape inventories are being managed appropriately and that the technology being applied is rendering their data unrecoverable."

SIMS SECURE SECOND WIN

Sims Recycling Solutions was named Secure Data Erasure Company of the Year for the second year in a row at the Computing Security Magazine Awards held in London in October. The award recognises its innovative ITAD services, guaranteed data erasure and superior customer service.

It was also runner-up in the category, Security Service Provider of the Year.

The company is the global leader in Secure IT Asset Disposition and Electronics Recycling Services. The services it offers allow organisations to manage their end-of-life mobile devices and IT equipment with the reassurance that their data is securely destroyed.

In March, it was also named Recycling Provider of the Year by industry experts at the Mobile News Awards.

Managing Director, Europe and India, Anand Narasimhan, said: "The secure IT disposition and data wiping services we offer are best in class and continue to develop in scope and value. We are thrilled to be recognised for these achievements and thank our clients and the readers of the magazine for taking the time to vote for us."

Recognised as a leader by top industry analyst, Gartner's 2015 ITAD Magic Quadrant, Sims Recycling Solutions offers sustainable global solutions which include on-site mobile data destruction, secure data sanitisation, value recovery through redeployment and remarketing as well as market-leading mechanical recycling and materials recovery delivered to clients at local, regional and global levels.

CALL FOR SUBMISSIONS

Contributions are welcome 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. Article size is generally 600-700 words per page, or for inclusion in the news section, 50-100 words.

Send to **magazine@adisa.global**

DOWNLOAD PREVIOUS ISSUES

The full archive of previous Adisa magazine editions can be accessed on our website: **adisa.global/adisa-magazine**


ADISA