The Emerging Issues of IT Asset Disposition: Data Security

القضايا الناشئة في التخلص والتصرف من اصول تكنولوجيا المعلومات: أمن البيانات

Dr Adel Ismail Al-Alawi,

Royal University for Women, Bahrain

Vice President of ISACA Bahrain Chapter

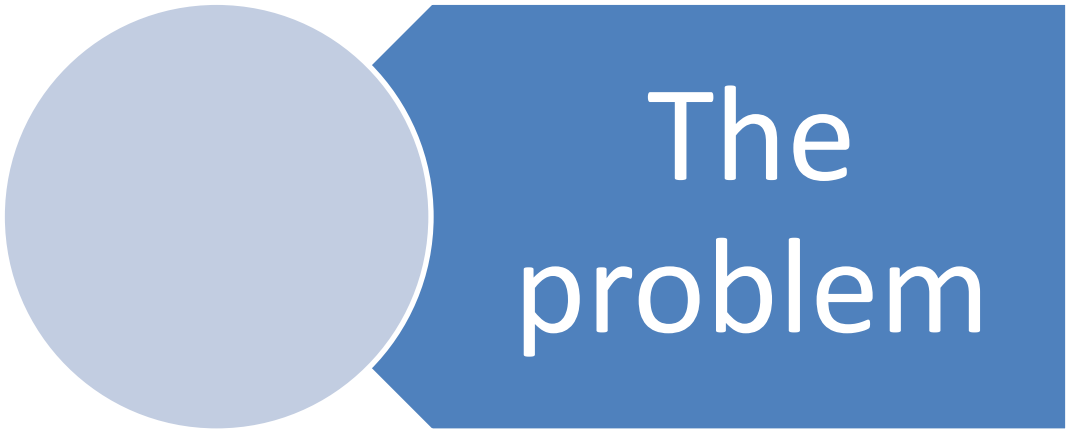
الدكتور عادل إسماعيل العلوي

الجامعة الملكية للبنات – البحرين

نائب رئيس الجمعية الدولية لضبط ومراقبة نظم المعلومات - البحرين

Agenda

- The problem
- Traditional Methods
- Case Study
- Recommendation


The
problem

What is E-waste???

Electronic waste or e-waste is the rapidly expanding volume of obsole

- computers,
- printers,
- fax machines,
- mobiles,
- TVs,
- photo copies
- other electronic devices

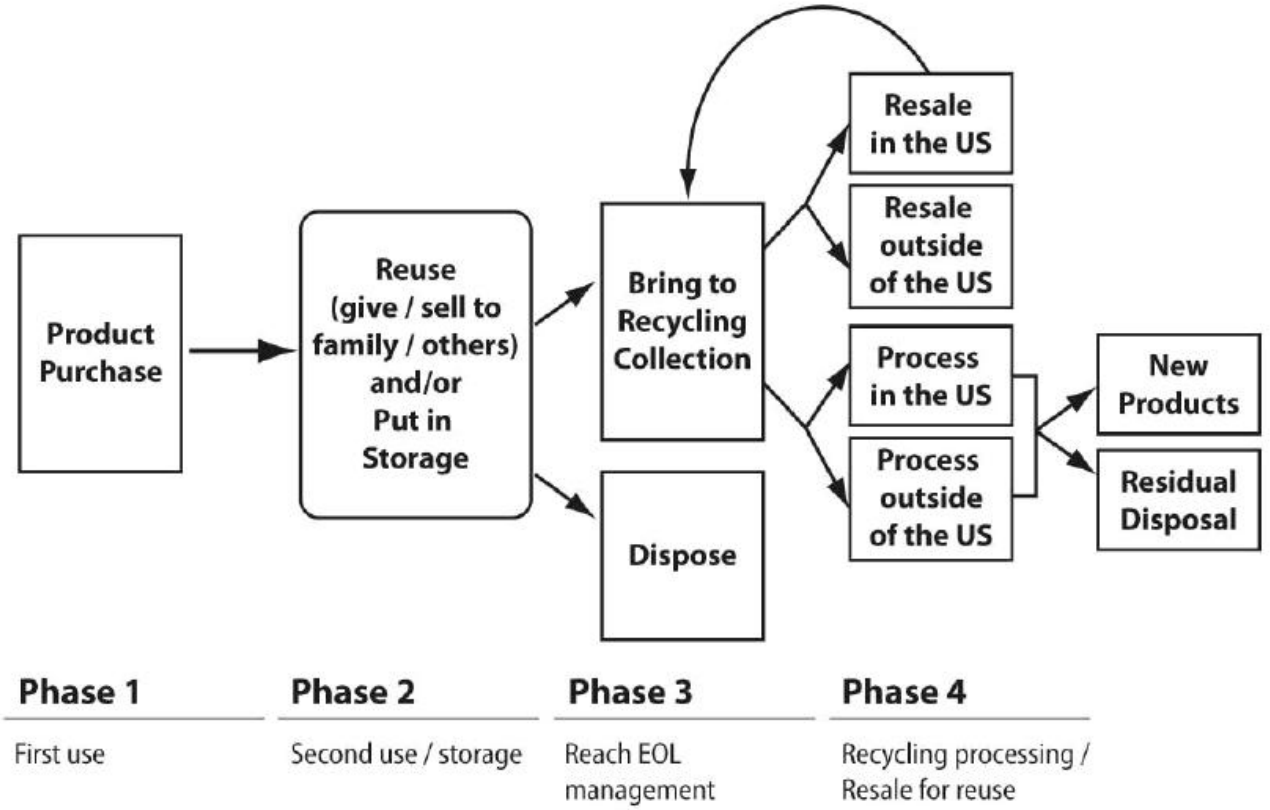
How Much E-waste Is There?

- e-waste is a recent phenomenon
  - **130 MILLION** cell phones discarded in the US in 2005
  - **60-65 MILLION** PCs become obsolete every year in the US
- Environmental Production Association estimate
  - **1.9 MILLION TONS** of e-waste landfilled in 2000 (EXCLUDING electric appliances)
  - **3 ~ 5%** of material in landfills growing **3 TIMES** the rate of other waste
  - **315 ~ 680 MILLION** computers/TVs waiting in "e-waste purgatory"

Where your Data is Stored?

- Hard Drives & Disks (ATA, USB, Zip disks, SCSI Drives, Magnetic Tapes, Floppies)
- CDs & DVDs
- cell phones, Blackberrys and other PDA
- Routers
- Copy Machines & Fax Machines

Private Data final destination



Ref. Richard Troia
i-recycle

Personal Record

- Personal Info
- Payment Info (e.g. Credit Card, Bank Account..etc.)
- Passwords
- Personal Correspondences
- Mission critical information
- Intellectual property
- Licensed software
- Personal Preferences/Behavior
- Other Personal Info (Pictures, family details, relations, medial info..etc.)

Business Records

- Today, 90 to 95% of all business records are stored in e-format & Paper represents <10% of all Business Records
- A single gigabyte of electronic storage has the capacity to store up to 75,000 typewritten sheets of papers.
- After 2 to 3 years of computer or BlackBerry use, it is easy to lose track of what information is stored – and where it is located.

Theft of Sensitive Information

2003 MIT Student Study:

- 158 used hard drives
- 129 still worked
- 69 had recoverable files
- 49 contained credit card, medical records & personal correspondence
- 1 contained ATM transaction info.

- One of the top areas for dumping e-waste is Africa
  - The number one area of the world for identity theft is **AFRICA!**


Traditional
Methods

The Benefits of Recycling the HD

- HDD is commonly known as Hard Disk Drive
- The primary device for storing all your data.
- One of the most expensive components in a computer (made up mostly of aluminum and other non-biodegradable materials).
- Provide us with highly reusable materials & protect the environment.
- Saving a portion of the cost associated with the laborious process by which the whole unit is assembled including the treatment of platters in order to attain a “mirror finish”.

HD recycling Barrier

- What happens when your info fall in the wrong hand
  - Utilize this info (Marketing, Competitors)
  - Identity Theft
  - Crimes (e.g. blackmail, financial transaction)

Is it easy to destroy files

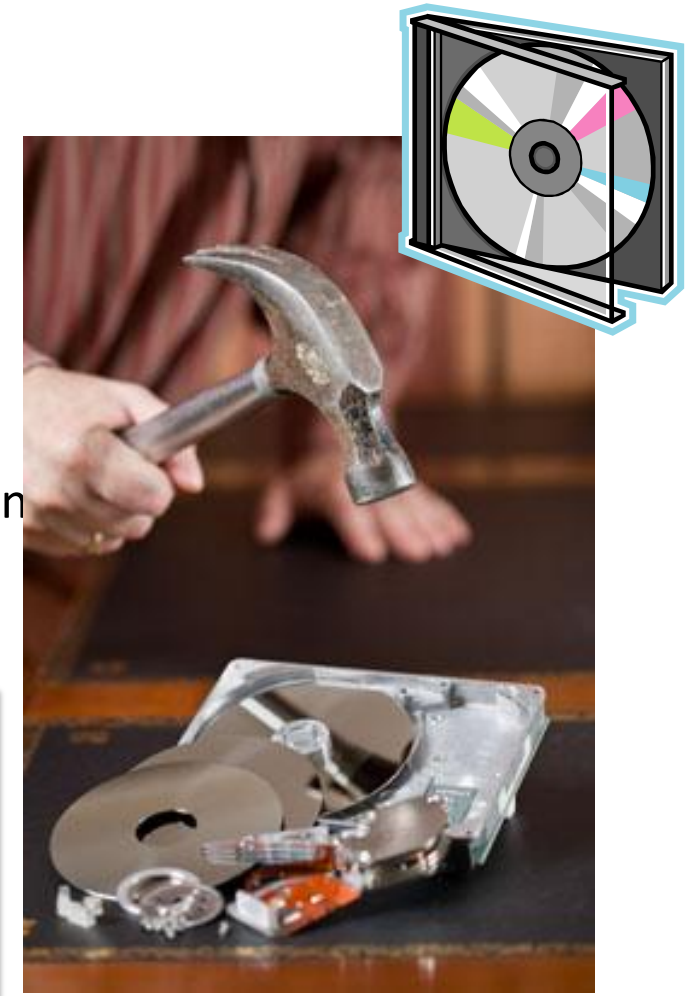
Ways to Try to Erase Hard Drive Data

- Is the Data Truly Gone?
- Simply Delete the File
- Empty the Recycle Bin
- Format the Hard Drive
- Repartition the Hard Drive
- Installing a new operating system

You need more than this !!!

Physical destruction

- Smash it with a hammer and use a hacksaw (Disintegrate & Pulverize).
- Grind it to dust (Incinerate).
- Burn it with acid.
- Shred



❖ Effective, **if** done correctly (100% destruction in seconds)

❖ Makes drive inoperable

• Time consuming,
• Flying debris
• Can't be recycled (Not environmentally friendly)
•Shredders are costly and not widely available

Software Destruction

- Meaningless pattern of 0's and 1's

❖convenient, and permanent

- **Maybe inaccurate**
- **Can't be used if media is damaged**
- **Need another hard drive to run the software**
- **Consume Cost, time and resources (days or weeks for few hundreds HD)**

Degaussing

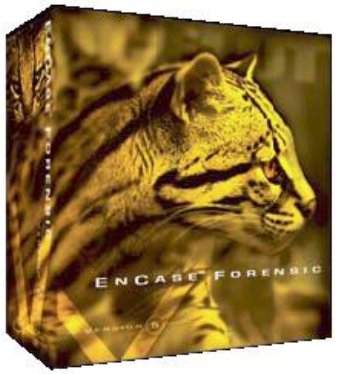
- Strong electromagnetic field

  destroys data

- **Machine expensive**
- **Not guaranteed to penetrate shield**
- **Hard drive cannot be reused**

Still Recovery is possible

- Data Recovery Software
  - EnCase
  - Forensic ToolKit
  - E-Mail Examiner
  - Many other specific use tools
- Data Recovery Hardware
  - Adapters
  - Write-blockers



Case Study

Glamorgan University Study

- A recent study by Glamorgan University (source: Time Online website) revealed more that 50% of 111 hard drives purchased contained personal and confidential information.
- Over 87% of those drives were bought from eBay.
- This may raises an international concern.
- While this is beneficial for the legitimated user, there is risk handling over our personal data to terrorists, and corrupt organizations, not to mention the risk of being blackmailed or threatened

Space Shuttle Columbia Hard Drive: How NASA Data was recovered after Crash

Timeline of Events

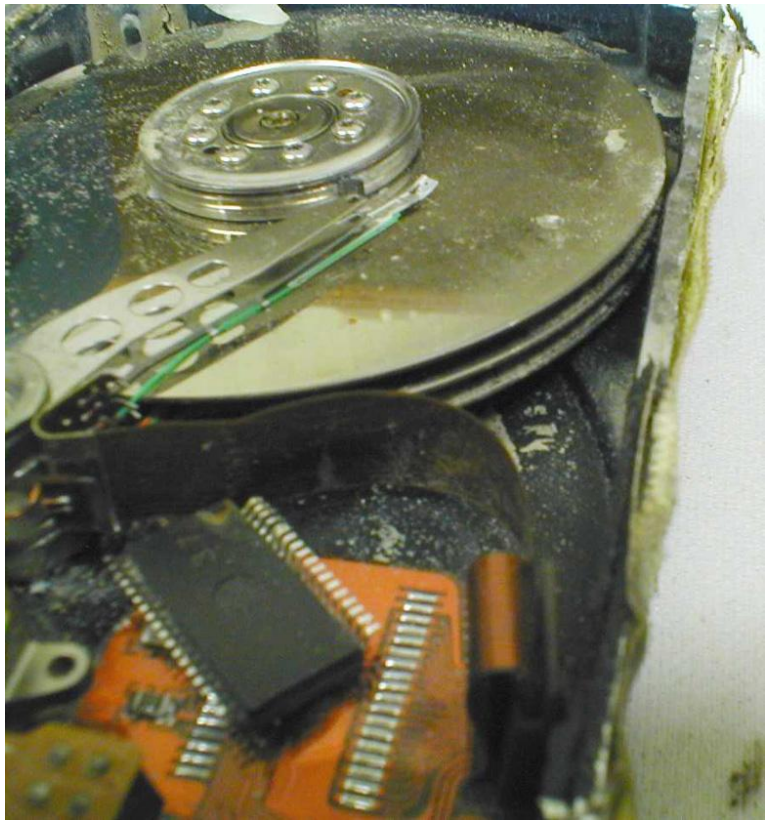
- February 1, 2003
  - Space shuttle Columbia disaster
- September 26, 2003
  - Ontrack Data recovery receives 3 drives recovered from debris
- September 29, 2003
  - Ontrack completes recovery of one of the disks
- April 17, 2008
  - Physical Review E publishes results of the experiment

Hard Drive Condition

- “Looked like a cracked hunk of metal” when it arrived for recovery.
- Every piece of plastic melted
- All chips burned and loose.
- Dirty and charred elements in the casing
- Everything but the platters were unusable.

Engineers worked to cut away protective top cover to get access to hard disk assembly

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9083478



Engineers then opened the top cover of the hard disk

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9083478

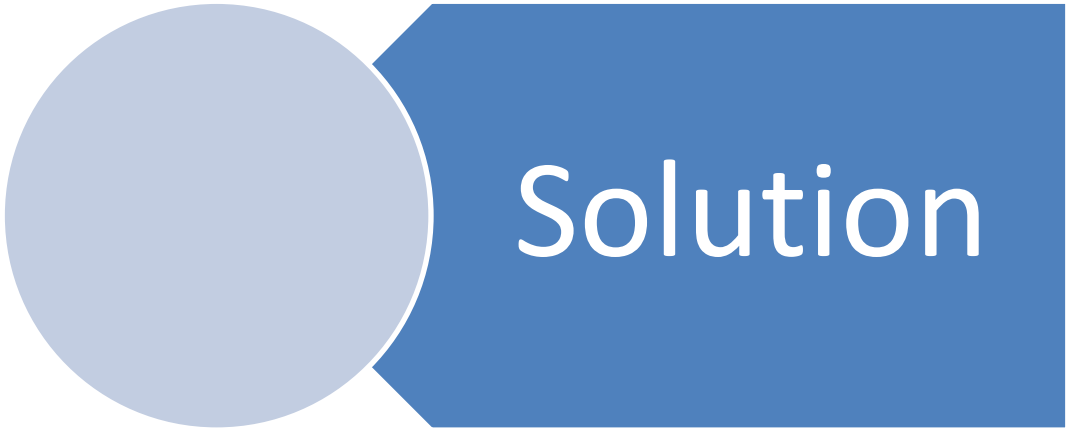
Engineers had to remove melted plastic from media and corroded, melted head assembly to remove each hard drive platter

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9083478

Recovery Details

- Platters were intact, but dirty.
- Cleaned the platters with special chemicals.
- Placed in a new enclosure
- Replaced the damage with minor adjustment
- Used custom software for data transfer that includes sophisticated error handling and calculations.

Recovered 99% of the data on the drive.


Solution

ATA principles of proper data destruction

- **A – Absolute:** With permission to destroy a record, destroy it in a way that it can never possibly be recovered under any conditions, including forensic data recovery techniques.

- **T – Timely:** Accumulation of data storage devices is a dangerous practice and should be minimized and all destruction events should take place on a scheduled basis avoiding ad hoc destruction activity that can lead to legal challenges as to the timing of the destruction event.

- **A- Auditability:** Must be able to prove that destruction activity is “routine” and done in “good faith”.

Monitoring & Control of Recycling firms

Provide assurance

Assurance

Independent Audit Firms

Expert

Confidence

Obtain confidence

Proof experience

Transparency

Solid & Transparent work environment

Accountability

Measurability

clearly defined policy

make **someone** responsible

Consequences of Non-compliance

- Loss of Public Trust
- Loss of Business
- Legal Fines
- Cost of Mitigation

Market Practice

- Individual Promises (DELL, HP, IBM, Nokia and others)
- Independent Authorities (e.g. NIST - National Institute of Standards and Technology)
- Other legislation such as
  - Health Insurance Portability and Accountability Act.
  - Sarbanes-Oxley Act.
  - Gramm-Leach-Bliley Act. (financial industry).
  - Family Educational Rights and Privacy Act (for educational institutions).
  - Fair and Accurate Credit Transactions Act.

Certifying Bodies

e-Stewards Initiative (e-stewards.org)

The e-Stewards Initiative is a project of the Basel Action Network (BAN), whic… 1(c)3 non-profit, charitable organization of the United States, based in Seattle, W… the backdrop of the growing e-waste crisis that the e-Stewards Initi… at appropriate national and international legislation or enforcement in… , it is unfortunately left up to individual citizens, corporations, univers… to figure out how to prevent the toxic materials in electronics from … g term harm to human health and the environment, particularly in countries … economies.

Provide the list of local/regional certifying body

The National Association For Information Destruction (N… D) offers a highly respected secure data destruction certifi… gram, which helps companies to find qualified pro… cure data destruction. NAID's mission is to promot… ation destruction industry and the standards and ethi… mber companies.

Certificate of guaranteed destruction

NAID AAA Certification For Secure Data Destruction

Sanitization Methods

- Clear
  - use software or hardware products to overwrite storage space on the media with non-sensitive data.
- Purge
  - Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains.
- Destroy
  - Disintegration, Pulverization, Melting, and Incineration
  - Shredding.

NIST GUIDELINES FOR MEDIA SANITIZATION

Media Type	Clear	Purge	Physical Destruction
ATA Hard Drives	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	1. Purge using Secure Erase. The Secure Erase software can be download from the University of California, San Diego (UCSD) CMRR site. 2. Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand.** 3. Purge media by using agency-approved and validated purge technologies/tools. **Degaussing any current generation hard disk will render the drive permanently unusable.	• Disintegrate. • Shred. • Pulverize. • Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.
USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks)	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	1. Purge using Secure Erase The Secure Erase software can be download from the University of California, San Diego (UCSD) CMRR site. 2. Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand.**	• Disintegrate. • Shred. • Pulverize. • Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.

Other Guidelines

- Keep records documenting :
  - Date,
  - Description & serial number,
  - Inventory number(s),
  - Process and tools used, and
  - Name/address of the organization receiving the equipment.

- Electronic records must be destroyed in accordance with records retention schedules.
- Those scheduled for destruction must be disposed of in a manner that ensures the protection of confidential information.

Middle East Status

No Certifying Body

ISACA Bahrain & Recycle IT Initiative

ISACA
Trust in, and value from, information systems
Bahrain Chapter

RECYCLE IT

Many Thanks

adel.alalawi@gmail.com

www.IsacaBahrain.gov