



Data Decommissioning: Overwriting, Shredding, Degaussing, and Beyond

November 18, 2008
ISSA-Minnesota Chapter Meeting
Minneapolis, MN

Agenda

- Introduction
- Data Doesn't Die
- Data Sanitization Methodologies
- "Secure Erase"
- COTS Solutions
- Q & A

Why Are We Here Today?

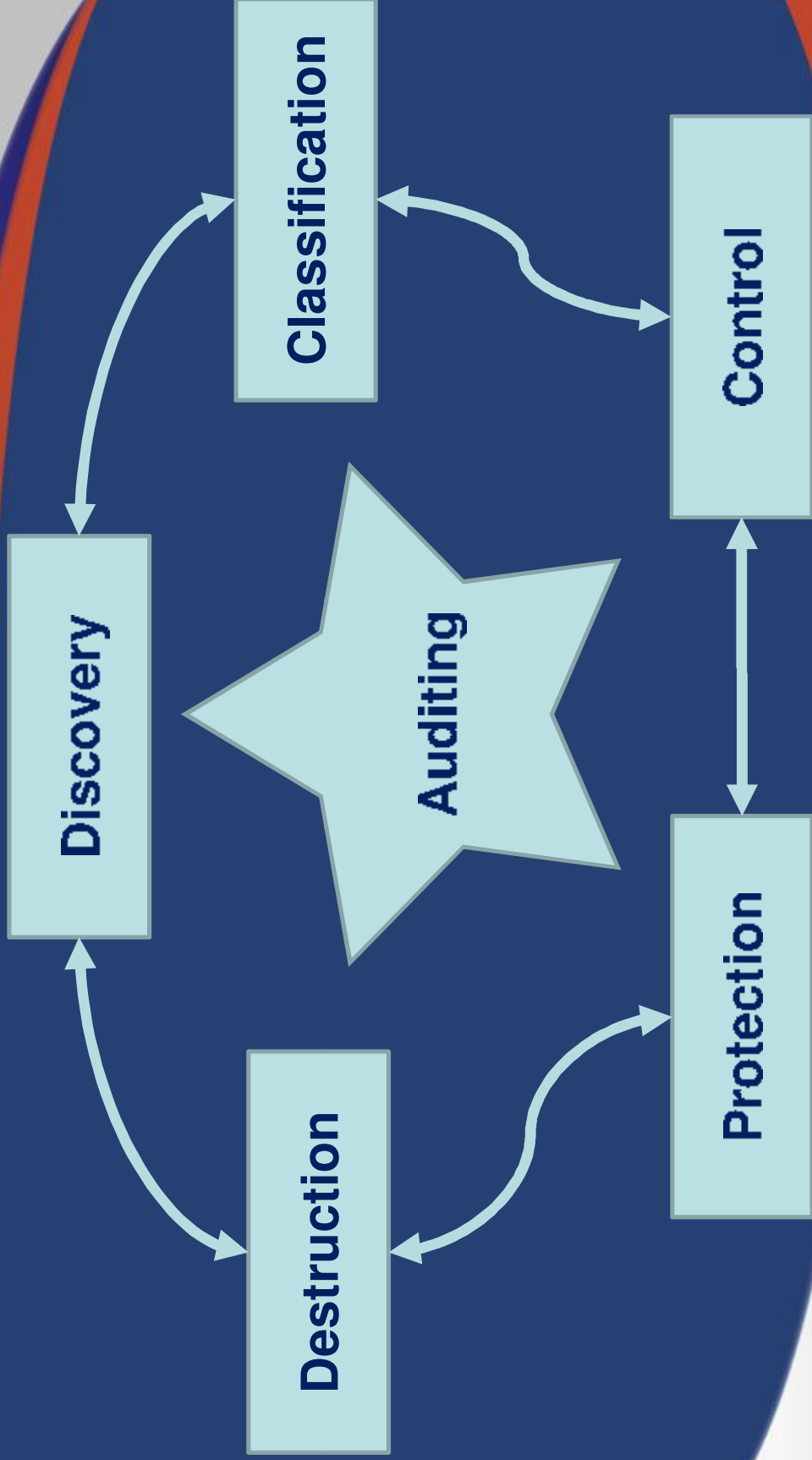
- Why is data sanitization important?
- Trends & new developments in data sanitization
- “Secure Erase” HDD firmware purge
- Care, custody & control considerations
- Recommendations / possible next steps

infoLock Technologies



- Headquartered in Arlington, VA
- Focus is **lifecycle data security** – understanding where sensitive data resides, how it moves through an organization, how it is used, and what risks it presents
 - Discovery, identification & classification of sensitive data
 - Data risk assessments, PCI-DSS auditing, policy/process improvement, encryption, authentication, access control, log & security information mgt
 - Proper decommissioning of data
- Clients across all regulated industries: financial, health, gov't, manufacturing, etc. – most < 500 employees
- Aligned with numerous security solution partners

The Data Lifecycle Challenge



Service Offering Overview



- Lifecycle Data Security from cradle to grave
- Security Consulting, Project Management, Solution Value Added Resale, Implementation & Training Services
 - Data Risk Assessments
 - Data Leak Prevention
 - Data Encryption
 - Laptop & mobile device encryption
 - Secure Messaging
 - Data Decommissioning
 - Vulnerability Assessments
 - Penetration Testing

Data Risk Assessment



- Monitor all outbound traffic to determine what sensitive data has left the organization
 - Via HTTP, SMTP, IM, FTP, Webmail, etc.
 - Data leakage through ports and devices
 - Includes all filetypes; structured and unstructured data
 - Who, what, where, and when?
- Scan storage locations to determine where sensitive data resides, and why?
 - Servers, file shares, desktops, laptops
 - What business policies are putting data in these location?
 - Are relevant security policies being adhered to?

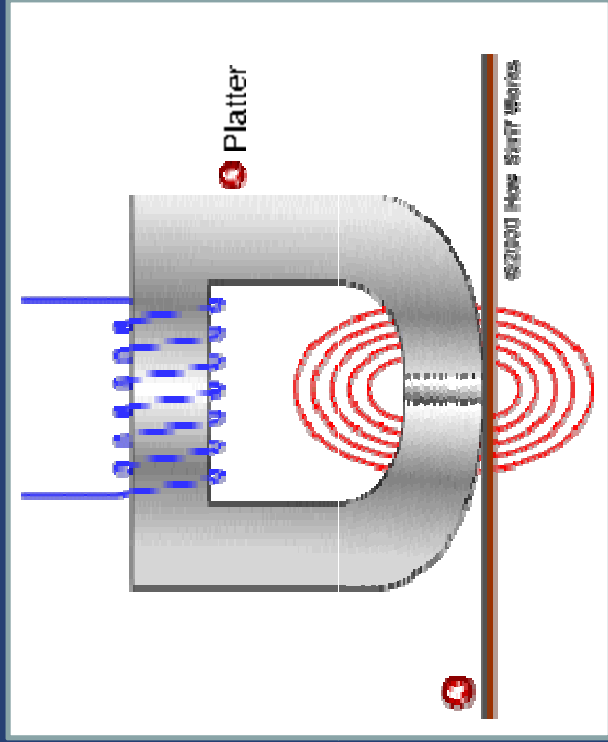
Data Encryption

- Laptops and Desktops
 - Full Disk, Folder and File level encryption
- Removable Media Encryption
 - USB Thumb Drives
 - External Hard Drives, iPods, Cameras, etc.
 - PDAs & Smartphones
 - CD/DVD
- Secure Messaging
 - Email encryption

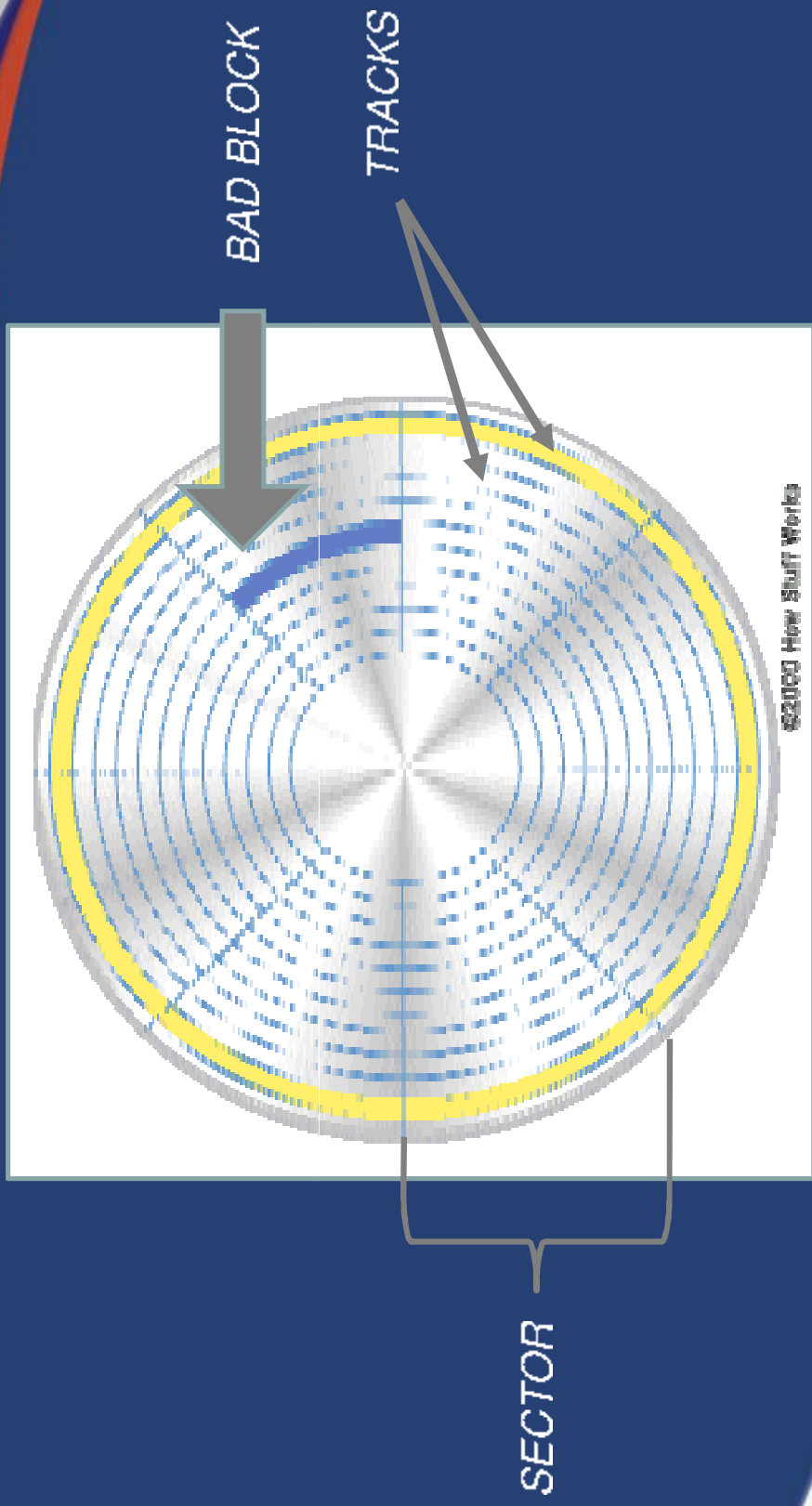
Hard Disk 101

- Hard disks developed in 1950s – termed “hard” to distinguish from “floppy” drives in use
- Modern hard disks are high-grade aluminum platters coated in *thin film* – a ferrous (magnetic) layer
- HDDs contain multiple platters, read/write heads, motors for spinning platters and moving heads, and embedded electronics
- Electromagnet read/write head applies magnetic charge to surface of hard disk “platter”, allows for re-writes
- Medium-term storage: 5-15 years?

Heads, Platters & Spindles



Hard Disk Terminology



Hard Disk Evolution



- Modern HDDs do not suffer from the “off track” magnetic write problems that characterized earlier models
- HDD operations are mediated by Operating System (OS) and higher-level software applications
 - Embedded firmware must be accessed by OS/apps
- HDD industry standards are often implemented slightly differently by manufacturers:
 - Seagate
 - Western Digital
 - Fujitsu
 - Maxtor
 - etc.

What You Know About...



**BANK OF AMERICA LOSES 1.2
MILLION CUSTOMER RECORDS**

**CHOICEPOINT IS FINED \$15.6 MILLION BY
THE FTC FOR PERSONAL DATA LOSS**

**VA LOSES 26.2 MILLION VETERAN'S
IDENTITIES**

FIDELITY INVESTMENTS LOSES 254K HP EMPLOYEE'S DATA

**AMERIPRISE FINANCIAL LOSES 226K CUSTOMER
AND EMPLOYEE'S DATA**

What May Be News to You...



GEORGIA STATE GOV'T - Surplus PCs sold containing hard drives with credit card numbers, birth dates, and SSNs of Georgia citizens.

IDAHO ELECTRIC UTILITY - 4 company hard drives sold on eBay contain hundreds of thousands of confidential company documents, employee names

MARATHON OIL - University student purchases recycled PC from eBay; hard drive contains PII and corporate IP of Texas company.

AICPA (American Institute of Certified Public Accountants) - Hard drive containing names, addresses and SSNs of 330,000 members lost when shipped back to AICPA by a computer repair company.

Public Exposure & Impact



Data Loss Impact

~ \$195 Per Record Compromised

- **Direct costs - \$30-50 per customer**
(Legal, notification, etc.)
- **Indirect costs - \$5-25 per customer**
(Lost employee productivity)
- **Opportunity costs - \$55-120 per customer**
(Loss of customer and recruiting new ones)
- **Government fines & penalties**
- **Exposure to legal action**
- **Shareholder value loss**
- **Diminished goodwill**



Cost of 3rd Party Data Breach



Average cost per record
compromised in 2007:

\$195

Average cost per record
compromised in 2007 by
Third Party:

\$238



Incident Response Elements

- free or discounted services
- free credit monitoring
- lost business
- notifications via email, letters, web, media, etc.
- legal defense costs
- criminal investigations
- legal audit / accounting fees
- call center expenses
- PR costs
- internal investigations
- security consultants

Source: Information Institute

Value of a Single Hard Drive?



- A Symantec report suggests that an ordinary laptop holds content valued at \$972,000, and that some could store as much as \$8.8 M in commercially-sensitive data and intellectual property
- Is this figure too high?
- Do we understand the value of our used hard disk drives?
- “An ounce of prevention...”

Half a Billion Hard Drives...



510 Million
Hard Drives
Shipped in 2007

17%

EXPECTED IN 2008 -
600 MILLION

Source: iSuppli

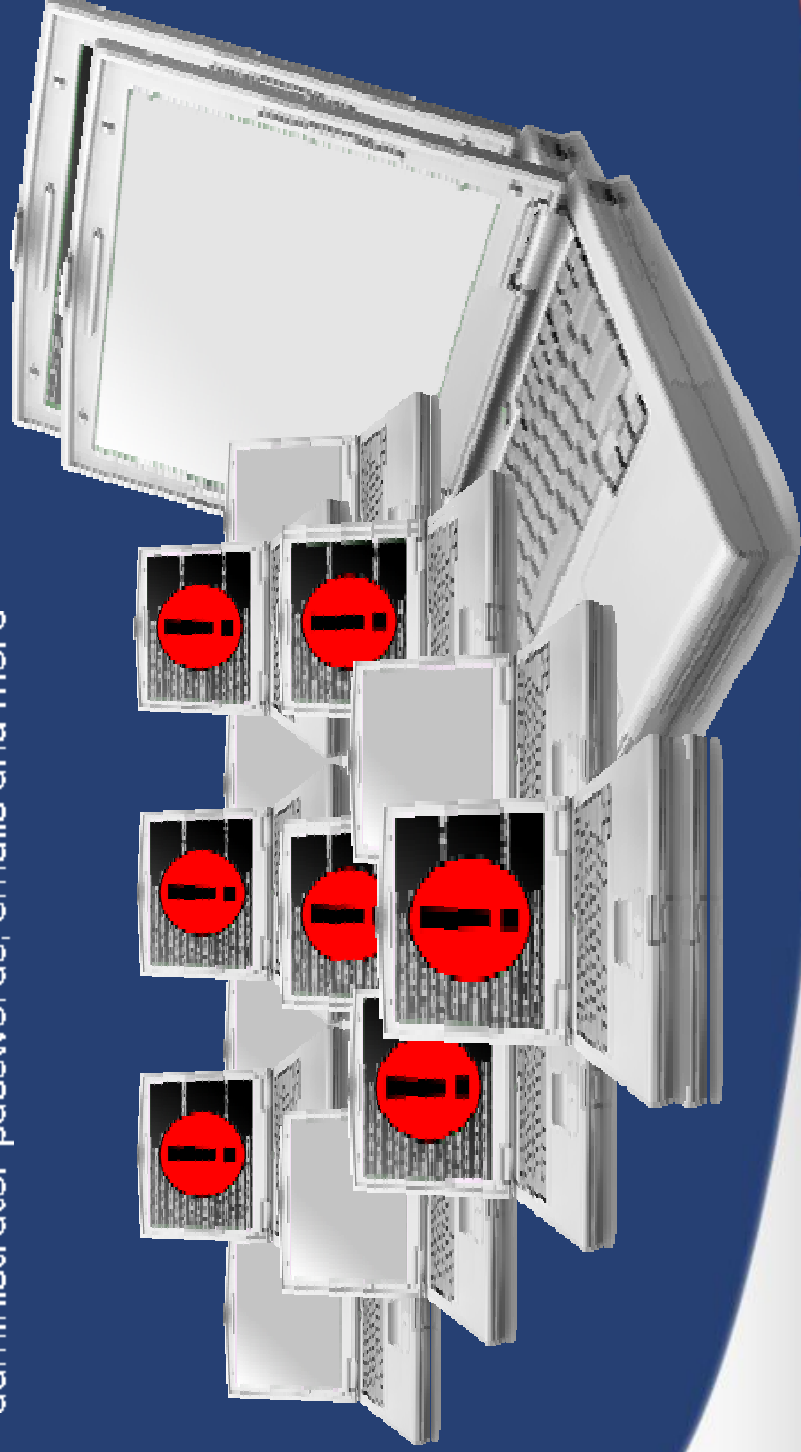
How Many HDDs are Out There?



BILLIONS?

Data Doesn't Die

Garfield, former Intel supplier, recently purchased 230 used hard drives from a former Intel supplier. He was able to read data on 7 out of 10 devices, including company details, login codes, administrator passwords, emails and more.



When is Data Destruction Necessary?



- When PC is to be sold, donated, discarded or recycled
- Whenever a drive is re-configured
- Whenever drive is returned to a manufacturer for warranty repair
- After virus attack or hacking attempt, for complete removal of offending code from infected storage device
- When a hot spare was automatically placed into service, and then removed when the faulty RAID drive was replaced. In this case the hot spare should be erased, as well as the original failed RAID drive if the drive is still operational (replaced due to imminent failure)

Data Decommissioning Methods



Data Overwrite



Degaussing Devices



Mechanical Destruction



Third Party Providers

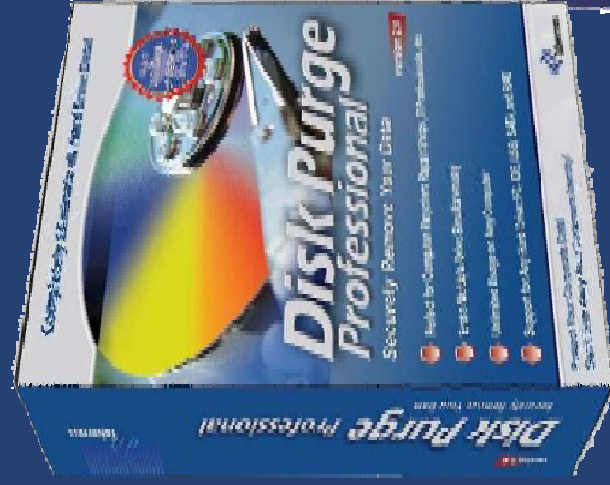
Approach #0: Data Delete

Uses Operating System to remove pointers to data on disk



Approach #1: Data Overwrite

Replaces existing data with a set of random or repeating data



Approach #1: Data Overwrite

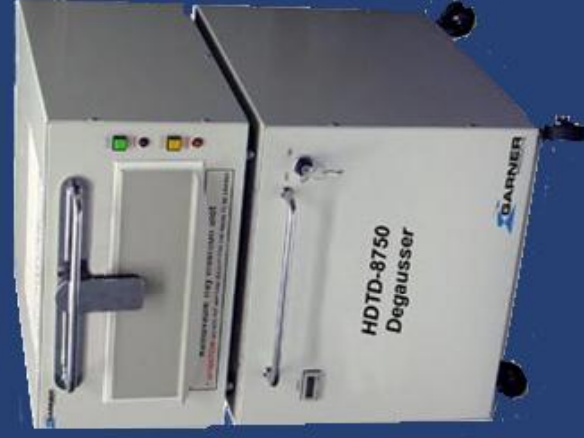


- Few if any ITsec practitioners in the DoD community will use methods compliant with DoD Standard 5220 for data overwrite for non-TS (unclassified) media
- Why? Because it doesn't eradicate data beyond forensic reconstruction
- DoD has adopted NIST's SP 800-88 guidance in this area of data sanitization, primarily degaussing & physical destruction

Approach #2: Magnetic Degaussing



Disables hard drive by applying a strong magnetic field



Approach #3: Mechanical Destruction



Reduces hard drive into scrap metal or physically disables the media

Mechanical destruction techniques include saws, hammers, nail guns, crushing mechanisms, belt sanders, mechanical shredders, etc.



Approach #4: Third Party Services



Third Party Services employ any of the previous methods...

The service may be performed on-site, or require that the hard drives be transported to the service provider's facility



Looking for a Another Approach



In the late 1990's, the international hard drive manufacturing community called a global summit to discuss the rapidly growing challenge of properly sanitizing hard drives.

Secure Erase is Born



HITACHI



TOSHIBA



Develop a means of sanitizing hard drives beyond forensic reconstruction while retaining the ability to reuse the hard drive.

The Hard Drive Industry collaborated with The Center for Magnetic Recording Research, under the direction of the US National Security Agency (NSA), to meet the challenge. They developed a sanitization standard called:

SECURE ERASE

Overview of Secure Erase



- A destruction command that is embedded in the firmware of ATA hard drives including IDE, EIDE, PATA, SATA, SCSI
- A single pass, atomic write operation that eradicates all data on the disk – beyond forensic reconstruction
- Up to 18x faster than DoD 5220 overwrite routines
- Hits all sectors of the hard drive
- Implemented by hard drive OEMs in 2002
- Validated and certified by various governing bodies of the International Security Community



Secure Erase – Freeware

- HDDerase.exe v3.3 (Nov 2007)
- Utilizes Secure Erase
- Authored by Gordon Hughes at the Center for Magnetic Recording Research (CMRR) at the University of San Diego
- Performs basic, “Proof of Concept” style Secure Erase operations
 - No audit trail
 - No format/re-image
 - No cert. printing
 - Cannot perform parallel purges
 - Requires a PC



Secure Erase – COTS #1

- Utilizes Secure Erase and is able to do overwriting for non-SE HDDs
- *Digital Shredder* from New Hampshire-based EDT
- Allows for purging, clearing (data overwrite), formatting & re-imaging
- Up to three (3) IDE/S(P)ATA/SCSI drives at once
- Audit, certificate printing, export logs
- Uses “personality blocks” instead of cables to connect drives



Secure Erase – COTS #2



- Utilizes Secure Erase and can perform overwriting for non-SE HDDs
- *Hammer* from Florida-based CPR Tools
- Allows for purging, clearing [data overwrite], formatting & re-imaging
- Up to four (4) SATA/PATA drives at once [can be daisy-chained up to 4x]
- Audit, certificate printing, export logs
- Cables connect to drives

Questions & Discussion



- There are many at-risk hard drives out there, with sensitive data
- It's important to destroy sensitive data whenever you relinquish care, custody or control of a hard drive
- There are at least 4 different approaches commonly in use today for data destruction:
 - Block overwrite
 - Magnetic degaussing
 - Physical or mechanical shredding
 - Secure Erase
- Data deletion or O/S reformat is *not* an option for data destruction
- For NIST compliance, physical destruction, proper degaussing, or Secure Erase purging are approved purge methods

For More Information

- **US National Institute of Standards and Technology (NIST) SP 800-88: Guidelines for Media Sanitization**
- NSA Information Assurance Advisory Alert – Authorization NO. IAA-00-2004
- US Deputy Secretary of Defense Memo dated May 29, 2001; Disposition of Unclassified DoD Computer Hard Drives, by Paul Wolfowitz
- US National Computer Security Center (NCSC-TG-018); Rainbow Series "Light Blue Book" - Guide to Understanding Object Reuse in Trusted Systems
- US National Computer Security Center (NCSC-TG-025); Rainbow Series "Forest Green Book" - Guide to Understanding Data Remanence in Automated Information Systems
- National Institute of Standards and Technology (NIST) SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems
- US Air Force System Security Instructions 5020
- US Army AR380-19
- US Navy Staff Office Publication (NAVSO P-5239-26)
- US Navy OPNAVINST 5239.1A

Contact Information

Sean Steele, CISSP, CISA
Sr. Security Consultant
703-504-9000 x219 direct
202-270-8672 mobile
ssteele@infolocktech.com

