

# PFIC



**Paraben's Forensic Innovations Conference**

**Park City, Utah**

**November 8<sup>th</sup>-11<sup>th</sup> 2009**



## BEST PRACTICES FOR THE DESTRUCTION OF DIGITAL DATA

Ryk Edelstein, Partner  
Converge net Inc.



# Converge Net

Established in 1991 as Montreal based outsource solution provider.

Specializing in the delivery of security and network efficiency solutions.

# Why Destroy Data?



- **Best Practice**
- **Regulatory Compliance**
- **Protection of Sensitive or Tactical Information**
  - **Personally Identifiable Information**
  - **Financial / Transaction Data**

# Potential Consequences

**Failure to properly decommission hard drives**

**Can lead to potential, catastrophic consequences:**

- Civil and criminal penalties
- Irreparable harm to reputation
- Lost confidence of client base
- Erosion of income and profits



# Why write a guide?



- Most published guidance does not have an expiration date, and is often orphaned as it goes EOL
- Policy authors are challenged when discerning fact from fiction
- No other (publicly available) comprehensive guide is available or accessible.

# CONSIDERATIONS



- **MOTIVATION /REASON FOR SANITIZATION**

- **DATA CLASSIFICATION**

- **HARDWARE SPECIFIC CONSTRAINTS**

# Considerations - Classification



- Who is the owner of the information?
- What level of data security classification has the device been exposed to?
- Is there decommissioning policy defined by class?
- Will the device to be reused or sold?

# Considerations - Hardware



What are the proper means to deal with drives with various interface types.

- SCSI (FC, SAS, Etc.)
- ATA (IDE, ATA,PATA, SATA)

Does the process address Protected Service Areas

- Host Protected Area
- Device Control Overlay
- Bad Data Blocks

Is the age of the drive a concern?

# Objective

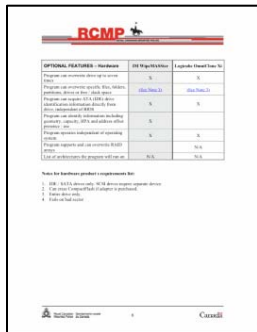


- **Best practice for the destruction of end-of-life data based on reliable and current practice**
- **Reliable, efficient and easily accessible technology**
- **Limitation of liability**
- **Standards based solution**
- **Green Solution**

# INTERNATIONAL REGULATORY GUIDANCE



**US National Institute of Standards and Technology**  
Computer Security NIST Special Publication 800-88



**Royal Canadian Mounted Police**  
Canadian Government Policy and Procedures for Media  
Sanitization B2-002 and ITSG-06



**Australian Department of Defence (ACSI-33)**  
Intelligence, Security and International Policy Defence Signals  
Directorate - Information and Communications Technology Security  
Manual

FIVE CRITICAL REQUIREMENTS most often requested by IT Security Professionals.



- Eliminate Data **Beyond Forensic Effort or Laboratory Reconstruction Capabilities.**
- **Absolute Care, Custody and Control** of the Process.
- Provide **Certification** that creates a **Defendable Audit Trail.**
- Ensure that the **Process is Scalable** and **Easy to Implement.**
- Provide a **Green** Solution, **Reformat & Image** for Reuse.

# COMMON PROCESSES AND THEIR LIMITATIONS



- **Overwrite Technology**
- **Degaussing**
- **Mechanical Destruction**
- **Third Party Providers**

**CLEAR**

**PURGE**

**DESTROY**

**DESTROY**

**What about ...**

- **Key Destruction**

**?**

# Where does Encryption fit in?



Encryption is best suited for the protection of live data.

When protecting information classified to Secret and Top Secret levels, the destruction process employed must assure that data can not be recovered using current or future technologies or practices.

In many cases encryption is not considered suitable for securing End of Life data.

# OVERWRITE SOFTWARE

## DESCRIPTION:

- Replaces existing data with patterns of random or repeating data

## LIMITATIONS:

- Multiple pass process -decreases but does not eliminate potential data recovery, residual data remains on the drive that forensic efforts can recover
- Single drive can take more than 24 hours
- Lack of automated data logging, audit trails or certification labels
- No security protection during the erasure process
- Not a scalable solution
- Vulnerable to manipulation or mis-configuration of software parameters



## DESCRIPTION: LIMITATIONS:

- Disables a hard drive by exposing media surface to a strong magnetic field



- Not “office friendly”
- Potentially Dangerous - high level magnetic fields require special precautions
- Destroys read/write head - prevents verification
- Unable to reuse drive
- Not a **green** solution
- Lack of automated data logging, audit trail or certification labels

# MECHANICAL DESTRUCTION

## DESCRIPTION:

- Reduces hard drive into metal particles or physically disables the media
- Mechanical destruction techniques include hammers, nail guns, belt sanders, and mechanical shredders



## LIMITATIONS:

- Heavy, bulky and noisy equipment, not “office friendly”
- Requires special handling and precautions
- Lack of automated data logging, audit trail or certification labels
- Not a **green** solution, toxic hazards at shredding site and landfill
- Unable to reuse the drive
- The smallest resulting particle should be smaller than a single sector of data. Currently this particle size is smaller than 1/250”

# THIRD PARTY PROVIDERS



## DESCRIPTION:

- Third Party employs any of the previous erasure methods
- The service may be performed on-site, or require that the hard drives be transported to the service provider's facility



## LIMITATIONS:

- **Loss of care, custody, and control**
- **Storage problems exist between visits**
- **Risk of loss during transit**
- **High service and transportation costs**
- **Retention of liability - a handoff does not absolve liability**
- **As previously mentioned, degaussing and mechanical shredding have other limitations**
- **Unable to reuse the drive**

# The Need for a Standard



## CHALLENGE:

In the **absence** of an **enterprise level Secure Erase solution**, **billions** have been spent on **products, processes** and **outsourced** solutions that were **not effective, scalable** or **failsafe**.

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

# SECURE ERASE



- Concept was proposed by IBM in 1994 as a subset of the ATA interface specification.
- 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 to engineer a standards based protocol for the effective elimination of all data on hard drive media. The primary goals being to implement a standards based purge protocol to be embedded in the firmware of all hard drives, which would quickly and efficiently eliminate all data beyond forensic reconstruction. The result was the development and universal adoption of the **Secure Erase** protocol.
- Adopted in 1998 as a component of the ANSI T-13 ATA specification.

# OVERVIEW OF SECURE ERASE



- **A data purge protocol initiated by a command that is embedded in the firmware** of ATA/IDE and SATA hard drives.
- An atomic process that **eradicates all data** on the disk **beyond forensic reconstruction.**
- **Up to 18 times faster** than less-effective commercially available overwrite product
- **Addresses all sectors** of the hard drive.
- Is a **compliant, certified standards** based technology.
- **Implemented by all hard drive manufacturers in 2001.**
- **Validated and certified** by various governing bodies of the **International Security Community.**

# SECURE ERASE - DEPLOYMENT CHALLENGES



**BIOS, Hardware and Operating Systems  
block the ability to reliably initiate and use Secure  
Erase.**

## **HERE'S WHY!**

**User error could trigger activation when not requested.**

**Virus, malware or Trojan could result in activation of the command.**

**Any unauthorized use of Secure Erase  
would be catastrophic.**

# CONCEPTS



- **PROCESS MUST BE RELIABLE**
- **POLICY SHOULD RESPECT DATA CLASS**
- **POLICY MUST ADDRESS ALL TYPES OF DRIVE**
- **AVOID LIABILITY OF ASSET LOSS BY AVOIDING WAREHOUSING DRIVES**
- **AVOID HANDING UNPROTECTED ASSETS TO THIRD PARTIES OR CARRIERS**
- **GREEN SOLUTIONS DO NOT SACRIFICE RELIABILITY**

# Developing Data Destruction Policy



- Consideration for the age of the assets to be processed
- Respect the constraints due to interface technology
- Consideration of organizational security objectives
- Consideration for the concerns by the owner (or those responsible for the security) of the data
- Classification of the stored data
- Asset value
- Ecological initiatives

# APPLIANCE BASED APPROACH

As Secure Erase can not be reliably deployed as a software application.

Appliance based solutions are the only reliable means of deployment.

**Satisfies the Key Features** required by IT Professionals.



- **Secure Erase**
- **Overwrite**
- **On-site solution suitable for enterprise or service provider use**

# Questions?



To contact me or to request

the Best Practice Guide or White Papers

- **Best Practices for the Destruction of Digital Data**
- **The Limitations of Software Based Hard Drive Sanitization**
- **Data Loss Prevention**

Managing the Final Stage of the Data Life Cycle Model

I can be reached at: [ryk@converge-net.com](mailto:ryk@converge-net.com)

Or 1-877-205-6806 x297

Thank you