IT Data Destruction Risks vs. Rewards

Corey Dehmey
Director of Sustainability
AERC Recycling Solutions

Overview

- What is IT Data Destruction
- Risks vs. Rewards
- Review of Data Destruction Methods
- Process Controls for Successful Data Destruction
- Decision Points

WHAT IS
IT DATA DESTRUCTION?

IT Data Destruction

- Removal of all stored information on an electronic device to the point that it is irretrievable by conventional means.
- Shredding, Pulverizing, Smelting
- Degaussing
- Software Based Overwriting

RISKS VS REWARDS

Issues

Risks

- Identity Theft
- Loss of Private Information
- Loss of Intellectual Property
- Loss of Competitive Information
- Violation of Privacy Laws

Rewards

- Higher Resale Value
- Increase Green Results
- Brand Protection

Privacy Regulations

Laws and Regulations mandating proper management of information:

Sarbanes-Oxley Public Company Accounting Reform & Investor Act
Regulates accounting and information handling of all publicly traded companies to help prevent accounting fraud.
Penalties & Fines
•Directors and Officers per violation - $1,000,000.00
•Institution penalty per violation - $5,000,000.00
•Years in prison – 20

Gramm-Leach-Bliley Act (GLB) Financial Service Modernization Act
Ensures the security and confidentiality of customer records and information in the banking, credit, insurance, investing and financial services industries.
Penalties & Fines
•Directors and Officers per violation - $10,000.00
•Institution penalty per. violation - $100,000.00
•Years in Prison – 5 to 12
•Impact on operations – Cease and Desist
•FDIC Insurance – Terminated
•Individual fines - $1,000,000.000
•Institutional (civil fines) – 1% of assets

Health Insurance Portability and Accountability Act (HIPAA)
Regulates healthcare organizations in the secure electronic transmissions, secure storage and disposal of patient information.
Penalties & Fines
•Institution – 450,000.00 to $250,000.00
•Years in prison – 1 to 10
•Individual civil fines - $25,000.00

Fair and Accurate Credit Transactions Act (FACT Act)
Contains provisions intended to combat consumer fraud including identity theft by regulating the destruction of papers containing consumer information.
Penalties & Fines
•Institution - -$11,000.00
•Individual – civil fines

REVIEW OF DATA DESTRUCTION METHODS

Total Destruction

Includes machinery to degauss, shred, pulverize, or smelt

PROS

- Assures complete destruction of data
- Shredding or degaussing can be done onsite for hard drives

CONS

- Reduces value of equipment for resale
- Creates a waste stream with hazardous components
- May require manual removal of internal hazards before destruction
- Usually requires offsite destruction
- Creates need to manufacture more product

Sanitization

Overwrite data using software or manufacture device reset

PROS

- Reliable data destruction technique if properly executed and controlled
- Can be done onsite before equipment leaves your control
- Expense decreases with volume
- Increases recovery value of equipment
- Extends the useful life of equipment and reduces manufacturing needs

CONS

- Higher risk of inadvertent data disclosure if process is not controlled

PROCESS CONTROLS
FOR SUCCESSFUL
DATA DESTRUCTION

Off-site shipments

- Secure material in your own storage
- Secured locked containers to transport material
- Secured storage at destination facility
- Tracking by weights, quantities, or serial #'s with accounting for each at time of receipt and at time of destruction.
- Client witnessed destruction on-site or through video.

Software Process

- Use labels for visual indication of sanitization.
- Use logging features in software to account for successful completion of each device
- Verify successful completion with software verification pass
- Implement Quality Assurance process to validate each device successfully completed in the logs. Utilize a 2nd person for the QA to maintain separation of duties.
- Create individual responsibility and tracking of each device being sanitized.
- Inspect inside of equipment for multiple drives
- Have process and sampling of equipment independently verified

NAID Certification

The NAID Certification Program establishes standards for a secure destruction process including such areas as security, employee hiring and screening, operational destruction process, and insurance.

- To promote the interests and general welfare of the information destruction industry; to encourage efficiency and bring about improvement in such services; to *extend the scope of the industry*, and to encourage the use of the services provided by members by commerce, industry, education institutions, and government.

- To *create a wider recognition of the industry as meeting the needs of commerce, industry, education institutions, and government* and its role in protecting the confidentiality of information and records.

- To *conduct and promote such other logical activities that will enhance the economic growth* of the information destruction industry.

DECISION POINTS

Decisions

- Risk Tolerance of the Business
  - CIA vs. Joe's Automotive Repair
  - Full Destruction or Software Sanitization
  - Onsite or Offsite Data Destruction
  - Internal or Outsourced
- Total Cost of Ownership
  - Can you extend the product life
  - What is the right time to resell

Tools

- NAID Certification
  http://www.naidonline.org/certification.html

- NIST's Guidelines for Media Sanitization – Special Publication 800-88
  http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

Recommendations

- Design a good process with checks and balances
  - Physical Security
  - Separation of Duties
  - Labeling
  - Quality Assurance and Verification
- Audit your vendor's process
- NAID Certification?
- Onsite Portable HardDrive Shredder
- Consider all Electronics with Storage Capabilities

Questions?