The Challenges of Security, Data Recovery, and Data Disposal with Flash/SSD

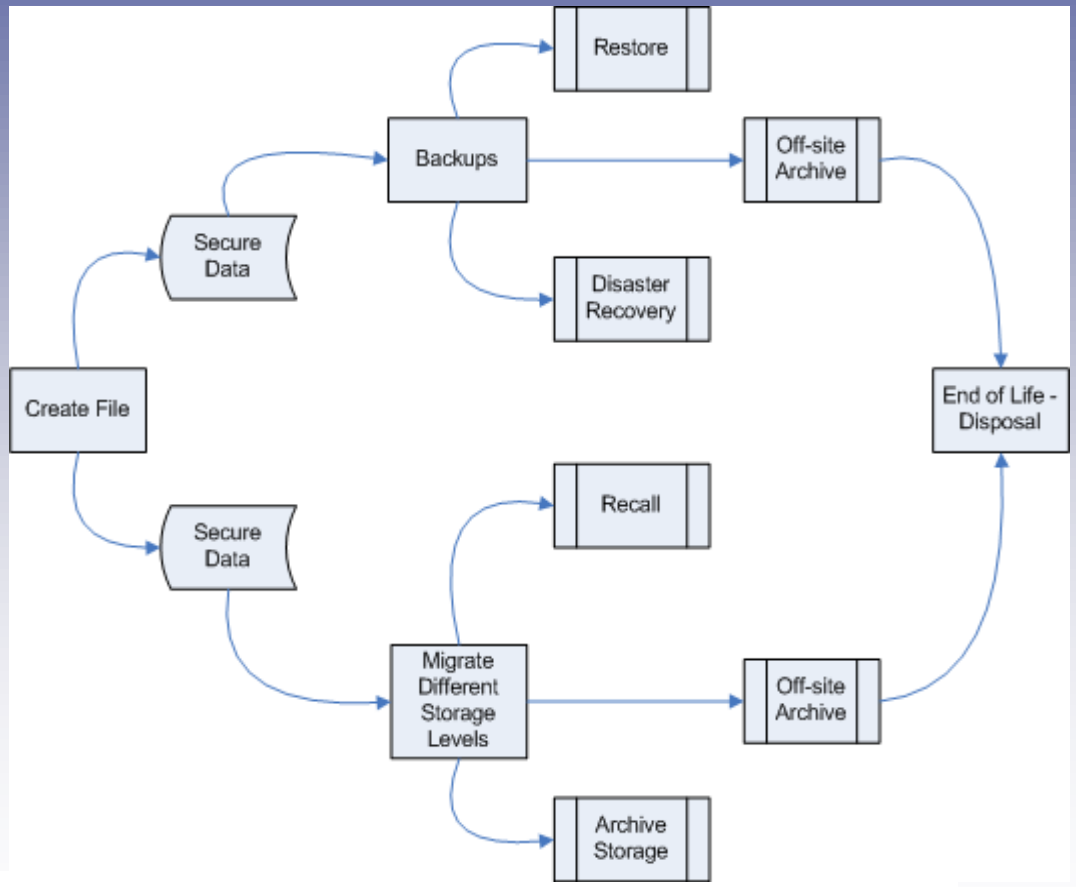
Sean R. Barry

Sr. Data Recovery Engineer

Kroll Ontrack

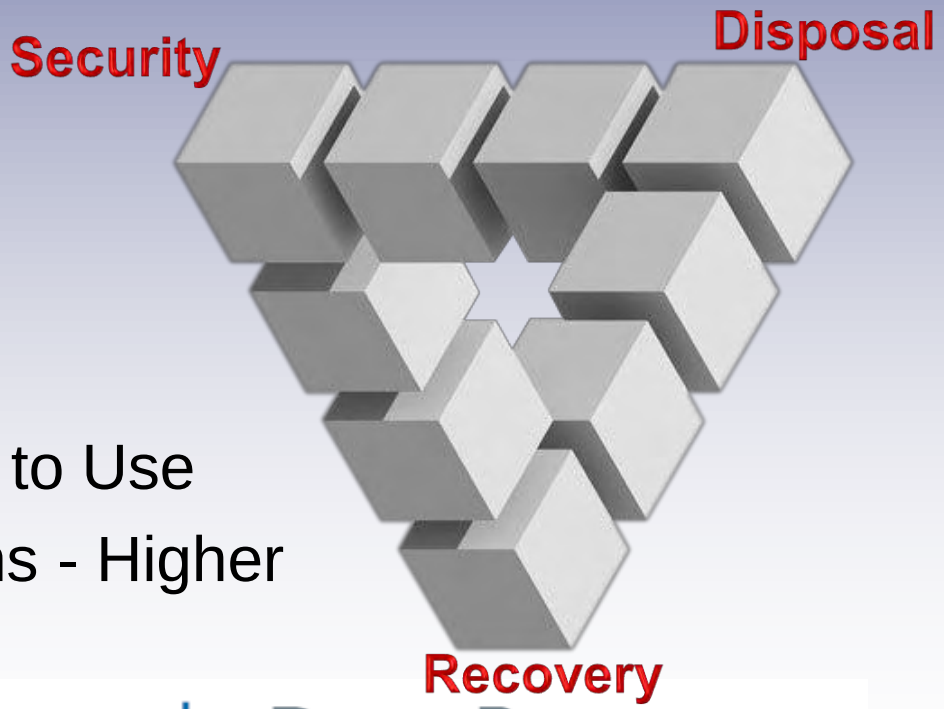
Lifecycle for Data

- Data Life Cycle
  - Data has a lifespan
    - Created
    - Backed Up
    - Migrated
    - Archived
    - Disposed
  - Data Center Storage Lifecycle



Lifecycle for Data on Storage Devices

- Flash/SSD Storage Devices – Just the Basics



- Flash Storage
  - Early Adoption
  - Enterprises Starting to Use
  - Storage Expectations - Higher

Storage Security, Recovery, Disposal - Example

Client Request for Complete Life Cycle Solution

18 working LUNs
12 backup LUNs
10 Blade servers
60+ TB of Storage
SAS and SATA drives

RAID 10 (1+0)
RAID 5

Cisco Switches and Firewall – 385MB of combined Flash Memory

Used with Permission

Security, Recovery, and Disposal of Flash Media - Options

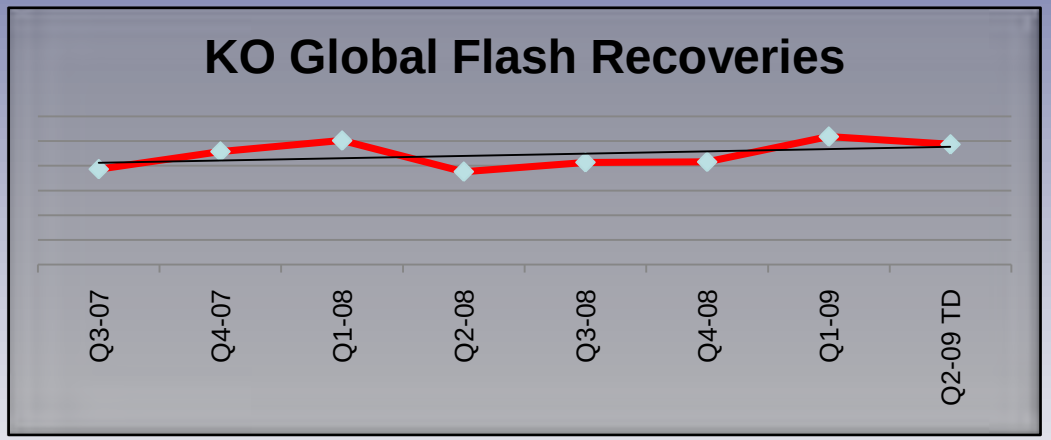
- Data Security
  - Physical Access
    - Small Form Factor— Risk of being lost, stolen, damaged

  - Data Access
    - User Enabled Encryption – File Level or Volume Level
    - Hardware Enabled Encryption – Full Device or Data Area

Security, Recovery, and Disposal of Flash Media - Options

Data Recovery

- Volume is Stabilizing
- Mix of SSD has increased over previous year



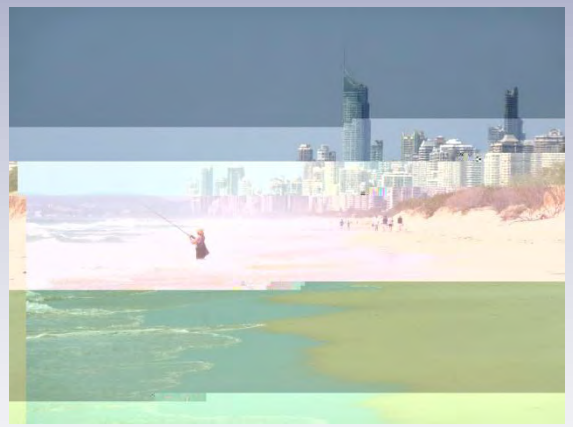
Process

– Device Triage – 20% of Flash/SSD Recoveries Can Be Fixed by Electronic Repair (Kroll Ontrack Statistic)

Security, Recovery, and Disposal of Flash Media - Options

- Data Recovery
  - Process
    - Data Extraction – ECC Risk; errors to the data stream

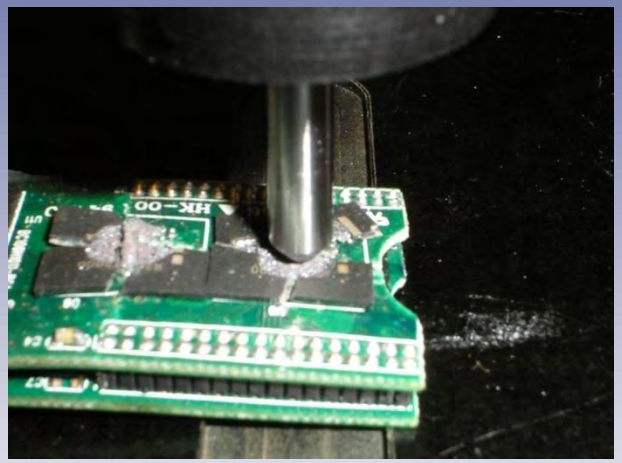
Not Client Data



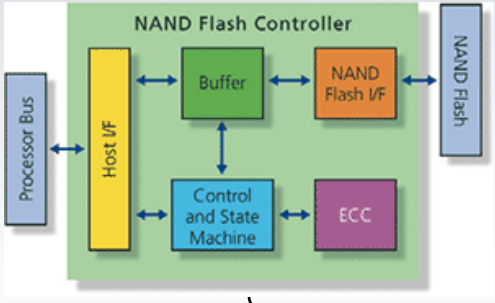
    - Data Assembly – Page, Erasure Block, Plane Mapping
    - Data Recovery – File System Repair; User File Recovery

Security, Recovery, and Disposal of Flash Media - Options

- Data Disposal
  - Destructive



  - Non-Destructive



Command Name	Command Code (HEX)
SANITIZE (including fast secure erase)	2H
SECURITY DIS	6h
SECURITY ER	3h
SECURITY	4h
SECURITY	5h

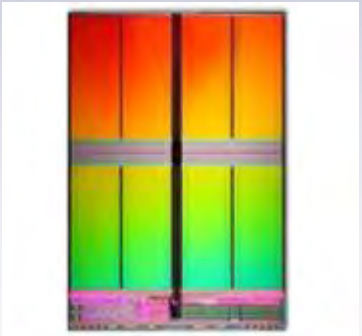
Challenges to Security Implementations

- **Passphrase and Key Management**
  - User forgets passphrase or is locked out
  - Part of decryption key is stored on media; when device fails, can't decrypt contents
- **Automatic Hardware Encryption**
  - Proprietary encryption engine part of controller microcode; when device fails, replacement controller is impossible for success
  - User doesn't know how to manage security

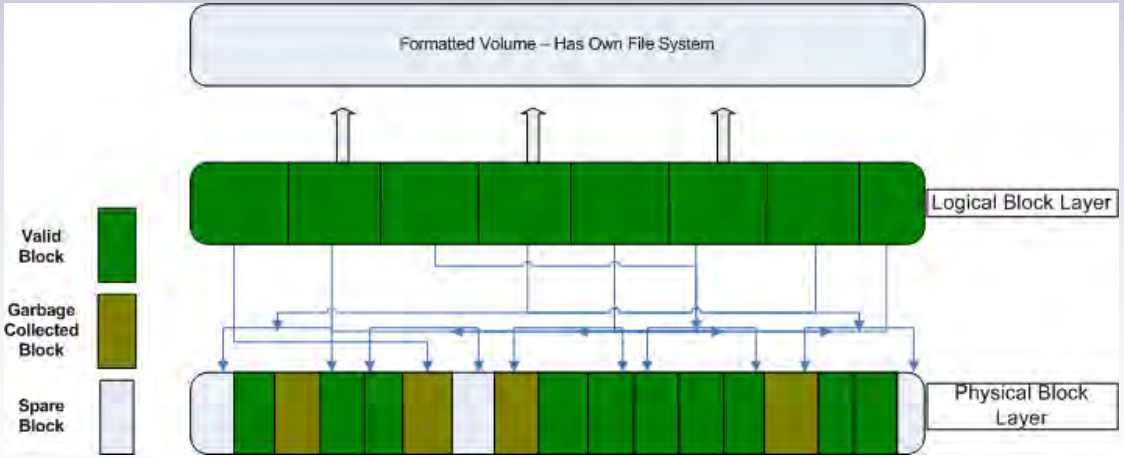
- Enterprise implementation requires a 'One Size' fits all Security method—for IT consistency
- Affects Data Recovery

Challenges to Security Implementations

- **Wear Leveling and Spare Blocks**
  - Extraction of raw data reveals user data in spare blocks
  - Blocks marked for erasure is not immediate – garbage collection delay
  - Corrupt blocks mapping prevents normal erasure process – leaves data intact and vulnerable



32Gb NAND flash chip; 34nm
Picture Credit: Intel

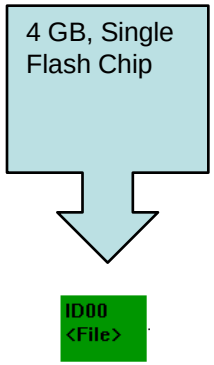


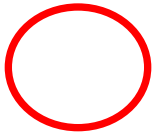
Challenges to Data Recovery

Device Properties	Challenge to Recovery
Proprietary Data Layout	Many Variations of Flash Translation Layer (FTL) Implemented
Address Line Complexity	Byte Inversion, Byte Striping, etc.
Wear-leveling Utilization	Wear-Leveling and Meta-Data Information Varies Widely

- No Consistency in Similar Product Lines or Models
- Increases Delays in Recovery
- Affects Consumer Perception of Reliability of Flash/SSD

Challenges to Data Recovery





Challenges to Data Disposal

- Enterprise Level
  - Data Destruction process in place—software based, logical volume overwrite
- SOHO Level
  - •Computer Tech to completely destroy data from a failed device?
    - •Most SOHOs are tech-savvy and try to do themselves
  - •Download “Free” software from Internet to Accomplish
- End User
  - •Does not understand risks
  - •Assumes that erased, formatted, overwritten means that it’s gone
  - •Uses it until device breaks or is damaged

Industry Course of SSD Data Security

- Security Options for Flash/SSD
  - Hardware Integrated Full Disk Encryption
  - Controller Sanitation Commands
  - Flash Cell Destruction (Overvoltage of Flash Chips; custom design—Be careful!)

Application and Take - Aways

Security

Fast and Secure

User Controlled

Enables Recovery

Ensures Disposal

Recovery

RAW Page or Plane Read

Controller Neutral

Disposal

Standard Sanitation Feature Set

Log of Operation

All Blocks Erased—Including Bad/Unused

Meeting Security Challenges

- Implement Security
- Provide for Recovery
- Design Disposal Features

- Complete Device Life Cycle Required for *All* Flash/SDD devices
  - Affects More Products—Build Confidence in Your Products by Including a Complete Solution