Data Recovery from Self-encrypting SSDs: The Benefits of Industrial Cooperation

Scott Holewinski, President

Gillware Inc.

scott@gillware.com

608.237.8784

Booth: 709

Setting the Stage

- **Fact 1:** People know the importance of backing up
- **Fact 2:** People don't back up
- **Fact 3:** SSDs can and **DO** fail
- **Fact 4:** Encryption works
- **Fact 5:** We live in a safety net society
- **Fact 6:** The Opal security spec and data recovery enablement don't mix

I don't necessarily believe this one to be true

Question I Want to Pose

Can the SSD and data recovery industries work together to develop a solution that would meet the public's demand for **data recovery from self-encrypting SSDs**, while still complying with the guidelines put forth in the **Opal security specification**?

Three Requirements to Recover Data from a Self-encrypting SSD

Requirement #1: Determine the NAND page layouts

Requirement #2: Determine the details of the Flash Translation Layer

Requirement #3: Ability to perform raw, unencrypted dump of NAND data

The State of SSDs Being Sent for Recovery

- Less than 5% electrical component failure
- 95%+ corruption to drive endurance mechanism (wear-leveling, garbage collection, etc.)
- Virtually **ALL** properly authenticate
  - 95% have no security password set
  - 5% with password set “panic” after password is entered

Requirement #3: Ability to perform raw, unencrypted dump of NAND data

Assuming the device can be properly authenticated

Thank You!

Scott Holewinski, President
Gillware Inc.
scott@gillware.com
608.237.8784
http://gillware.com
Booth: 709