SDC
STORAGE DEVELOPER CONFERENCE
SNIA SANTA CLARA, 2016

When Will Self-Encrypting Drives Predominate?

Tom Coughlin
Coughlin Associates

Walt Hubis, CISSP
Hubis Technical Associates

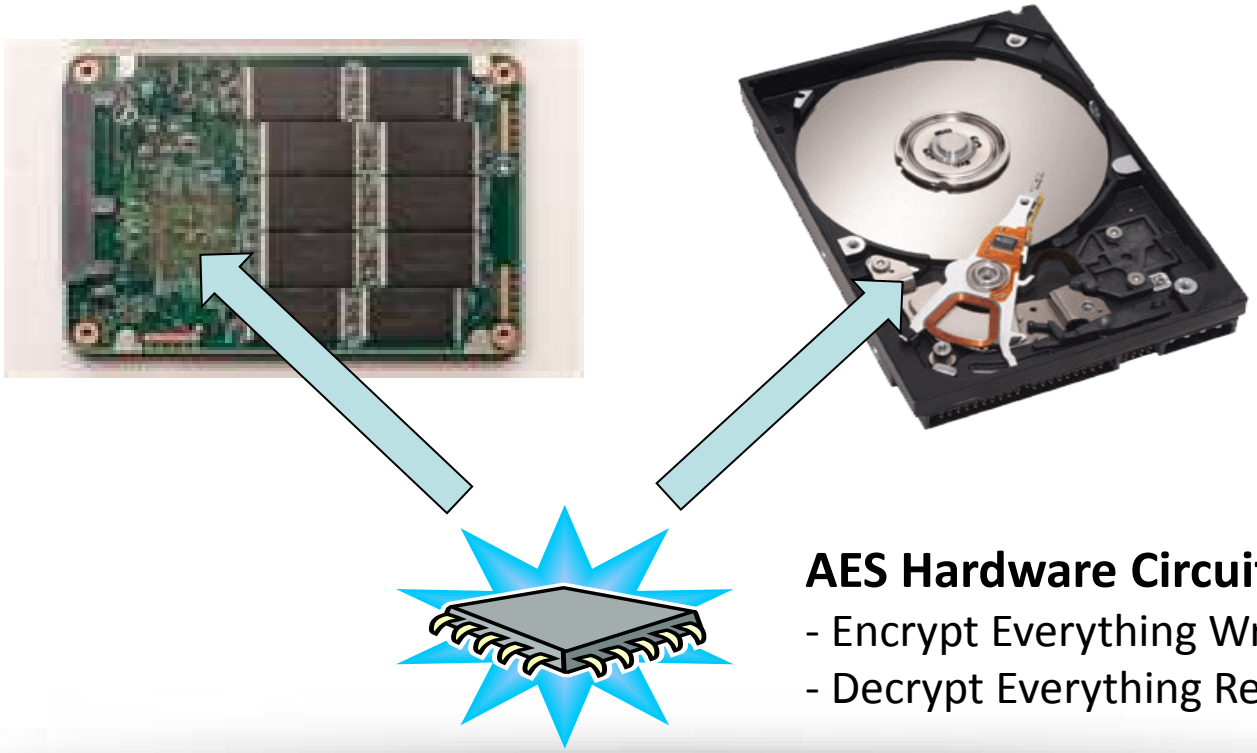
Abstract

Self-Encrypting Drives (SEDs) have found applications in enterprise storage where crypto-erase allows rapid sanitization of retired drives but their use in client storage devices is still minimal. Learn about the history and uses for SEDs and what needs to happen to bring them into broader use based upon results from a recent poll of client end users.

What is a Self-Encrypting Drive (SED)?

Trusted Computing Group
SED Management Interface

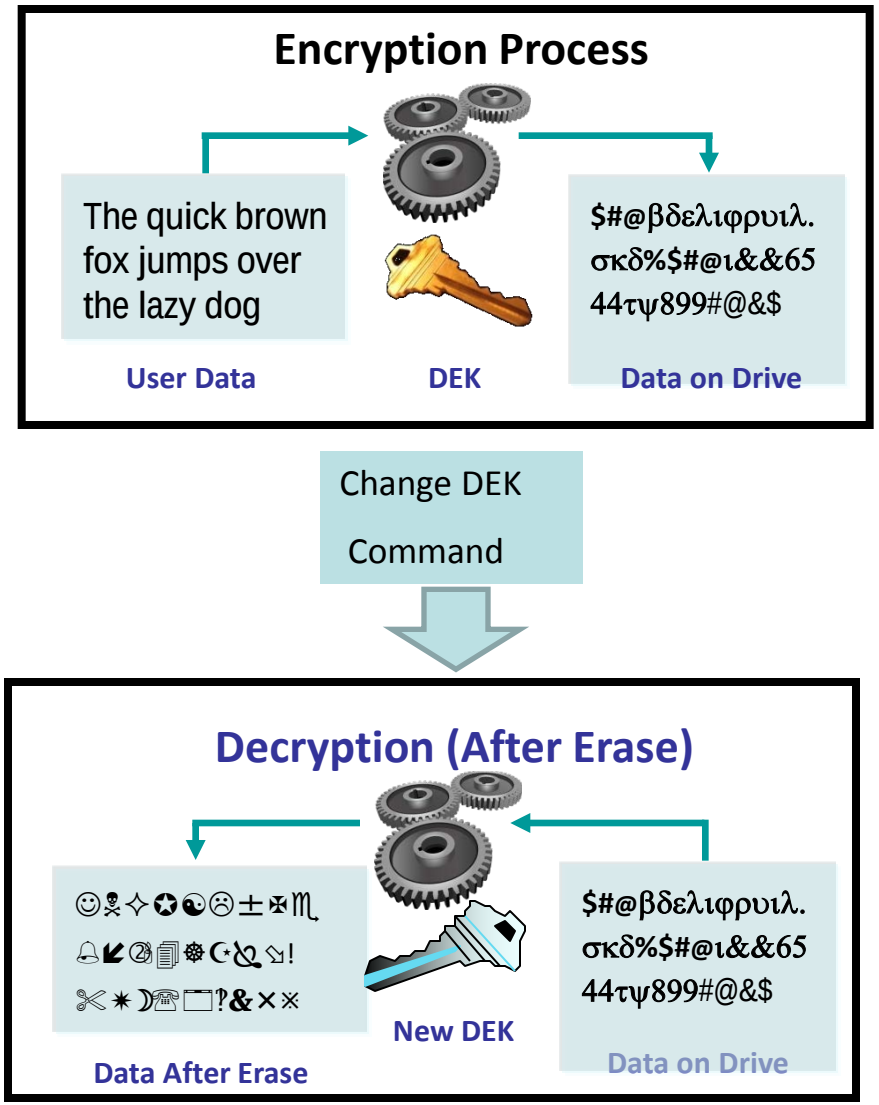
I n t e r f a c e



AES Hardware Circuitry
- Encrypt Everything Written
- Decrypt Everything Read

CRYPTO ERASE

- **Description**
  - Cryptographic erase changes the drive encryption key
  - Data encrypted with previous key, unintelligible when **DEcrypted** with new key
- **Benefits**
  - Instantaneous “rapid” erase for secure disposal or re-purposing



http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

Hardware-Based Self-Encryption vs. Software Encryption

- **Transparency**
  - SEDs come from factory with encryption key already generated
- **Ease of management**
  - No encrypting key to manage Life-cycle costs
  - The cost of an SED is pro-rated into the initial drive cost
  - Software has continuing life cycle costs
- **Disposal or re-purposing costs**
  - With an SED, erase on-board encryption key
- **Re-encryption**
  - With SED, there is no need to ever re-encrypt the data
- **Performance**
  - No degradation in SED performance
- **Standardization**
  - Whole drive industry is building to the TCG/SED Specs
- **No interference**
  - with upstream processes

New hardware acquisition (normal replacement cycle)

SED Updates

- Published by Coughlin Associates April 2015
- Authors
  - Walt Hubis: Technical Content
  - Tom Coughlin: Market Analysis
- Audience
  - Manufacturers
  - System Integrators
  - Security Analysts
  - Business Analysts
- New report out in October 2016

2015 Key Findings

- By 2017 we project that 100% of all HDDs shipped will be SED capable, driven by implementation of this capability into commercial HDD controllers
- By 2018 about 11% of all HDDs shipping units will shift to SED enabled promoted products, driven by security adoption demand.

2015 Key Findings

- By 2018 the high, median and low estimates for SED enabled adoption for SED HDDs are 85 M, 70 M and 54 M units.
- By 2014 almost all SSDs were SED capable and by 2015 they all have this capability.
- Although actual SSD SED feature implementation in 2018 is 100% in about 236 M SSDs, the projected actual SSDs from that year intended for security and data protection purposes is estimated at less than 24 M units.

What's Changed?

- Continued maturity of SED market
- Continued shift to solid state storage
  - Secure erase is important
- Maturity of NVMe security features
- TCG Maturity
  - Diversification of security interface specifications
  - Development of security compliance programs
- Impact of new threat reports
- Trends toward networked storage
  - NVMe over fabric
  - Kinetic

Hacks

- Bypassing Local Windows Authentication[1]
  - Haken, November, 2015
  - Patched shortly after
- Kaspersky Report[2]
  - February 2015
  - Master boot record attack
  - UEFI Secure Boot
- Power hack
  - Keep SED drive powered to access data
  - Proposals for heartbeat

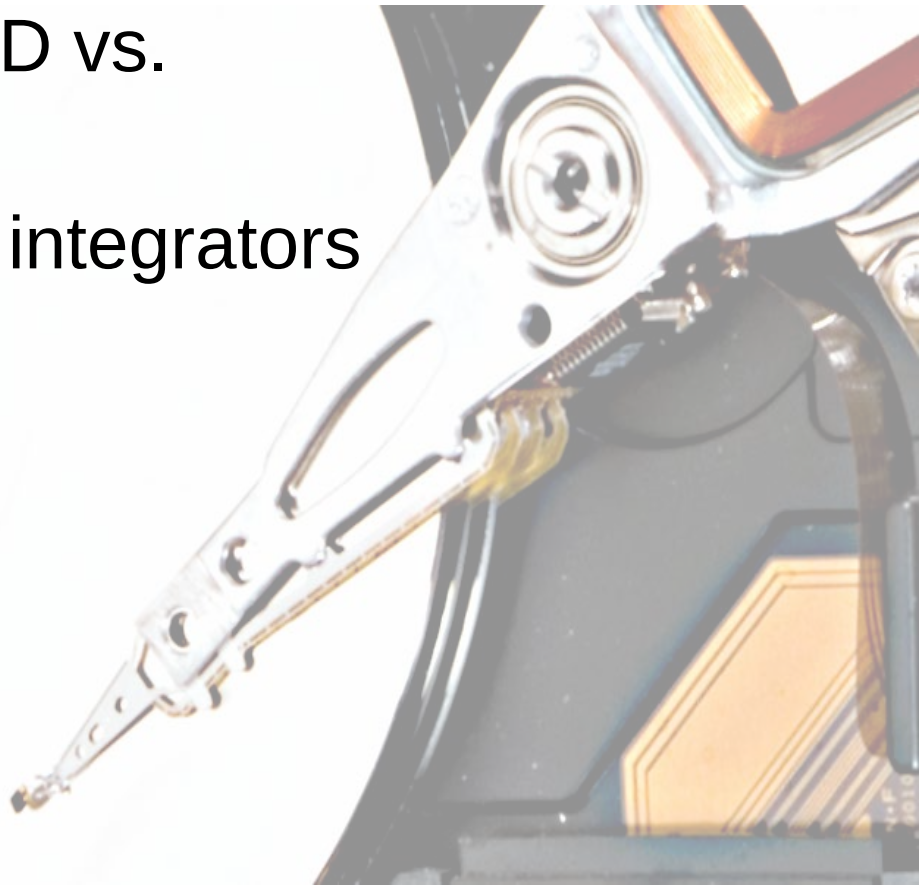
1) https://www.blackhat.com/docs/eu-15/materials/eu-15-Haken-Bypassing-Local-Windows-Authentication-To-Defeat-Full-Disk-Encryption-wp.pdf
2) https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf
3) Photo: http://www.theregister.co.uk/2015/02/17/kaspersky_labs_equation_group/

Loss of Trust

- Hacks have lead to a loss of trust in drive vendors
  - Even though no drive firmware attacks found
- Increasing visibility of malicious behavior
  - Recent hacks, purportedly by nation states
  - But not at the drive level
- Scope of enterprise security
  - Data at Rest is a small part of a huge problem
  - Database, file system, application encryption
  - Physical and administrative security

What's Needed?

- Understand drivers for SED vs. software encryption
- Understand end-user and integrators perspectives
  - Perceptions
  - Needs
- Certifications Status
  - TCG Opal Certification
  - Common Criteria
  - FIPs



Trusted Computing Group Storage Certification

Storage Certification

Storage Certification allows TCG members to demonstrate that their storage products meet a set of Compliance and Security Evaluation requirements that was developed with TCG membership and industry participation input. Storage products passing certification are listed on the Certified Products List. Storage certification is a benefit of TCG membership and therefore membership is required.

The certification requirements for a member's storage product to achieve TCG Certification include:

+ Storage Compliance Testing

The certification specification for the Opal SSC (Security Subsystem Class) is available on the TCG website. A Storage Certification Workshop is held to certify the test suites generated by the test vendors. Using a certified test suite, the storage device can validate the compliance of the implementation to the certification specification. Drive makers can become certified via one of three paths, which will only be available to members:

- A TCG-hosted storage compliance workshop
- Third-party test labs
- Self-certification
- Security Evaluation

TCG members are required to demonstrate successful Common Criteria certification based on Common Criteria Full Disk Encryption (FDE) Encryption Engine (EE) collaborative Protection Profile (cPP).

New Interface Architectures

- NVMe over fabric
  - iWARP and RDMA
  - Complex security
- Kinetic drives
  - Ethernet Interface
  - Key-Value
  - Transition to fully networked drives

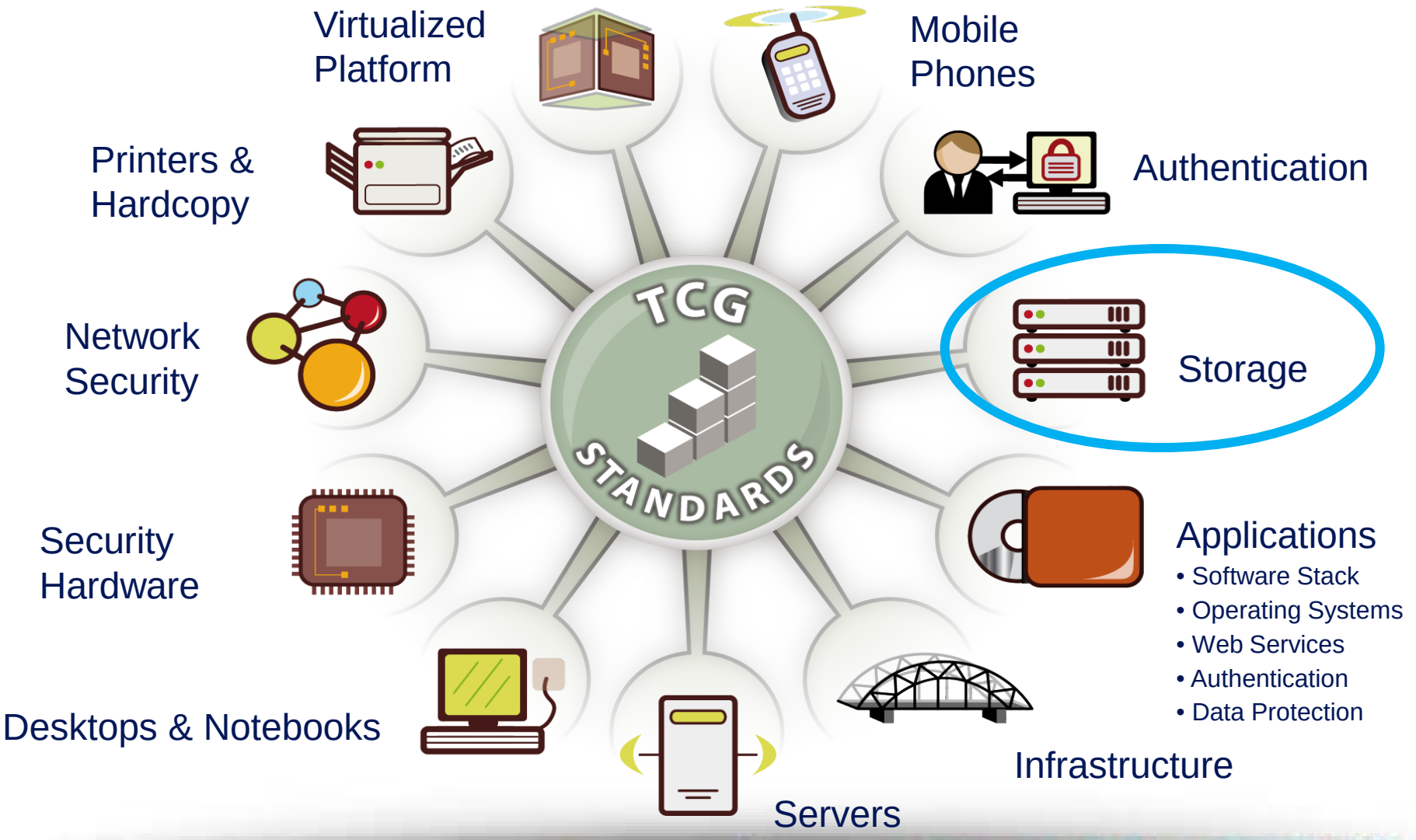
Trusted Computing Base

- Prerequisite to security
- Trusted software
- Memory protection
- Guaranteed resources
- Deterministic software
- Access controls
- Sandbox – process isolation
- Root of trust

Standardization

- TCG Opal Certifications
- Common Criteria
- FIPS 140-2
  - ISO/IEC 19790 : 2012
  - Information technology -- Security techniques -- Security requirements for cryptographic modules
- ISO/IEC 27040 : 2015
  - Information technology -- Security techniques -- Storage security

Trusted Computing Group Standards



Key Management

- Enterprise key management is crucial
- Key Management Standard
  - OASIS Key Management Interoperability Protocol (KMIP)
- Conformance
  - SNIA SSIF Key Management Interoperability Protocol Conformance Test Program

The Drive Trust Alliance

- The Drive Trust Alliance brings together the state of the art in SED technology. Storage Device Makers, Storage Security Software Vendors, IT departments, and just plain End Users will find how to employ SED technology to solve many of today's massive and serious data leakage problems.
- At the Drive Trust Alliance (DTA), we join our members in a commitment to growing the adoption of self-encrypting drives (SEDs) for the consumer market.

The Drive Trust Alliance

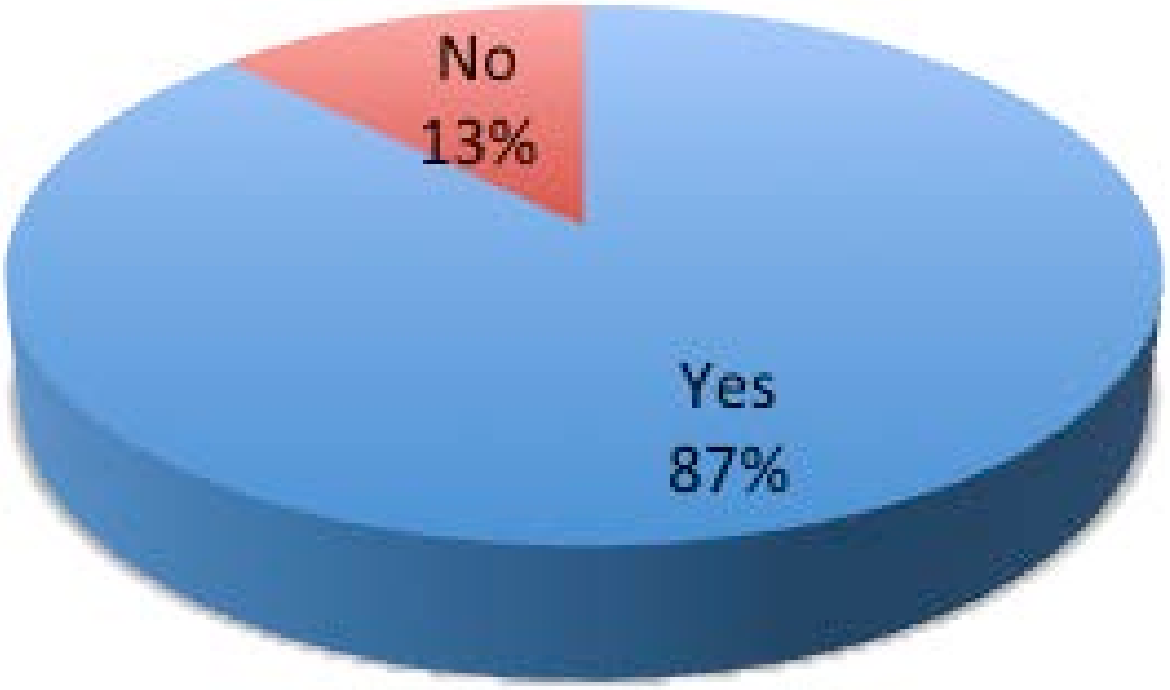
- Flash SSDs
- iPhones, iPads, Android
- All of Google
- All Printers
- Protecting “USER” Data
- **www.drivetrust.com**

Report Input Needed

- Input from end users and integrators
  - Perceptions and needs
- Input from drive vendors
  - Future directions and guidance
- Input from standards organizations
  - Future direction and time frames
- Help get end users to take the ongoing end user survey: https://www.surveymonkey.com/r/ZDGP7HM
- Preliminary survey data follows

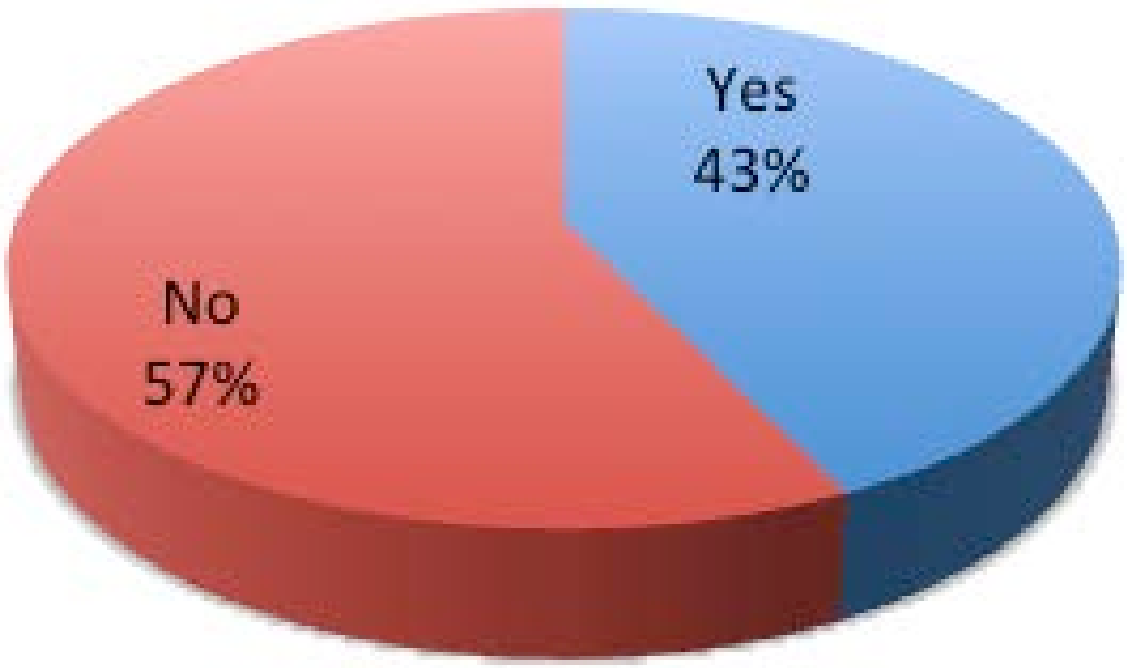
Report Results

Are you familiar with self-encrypting drive (SED) hard disk drives and/or solid-state drives?



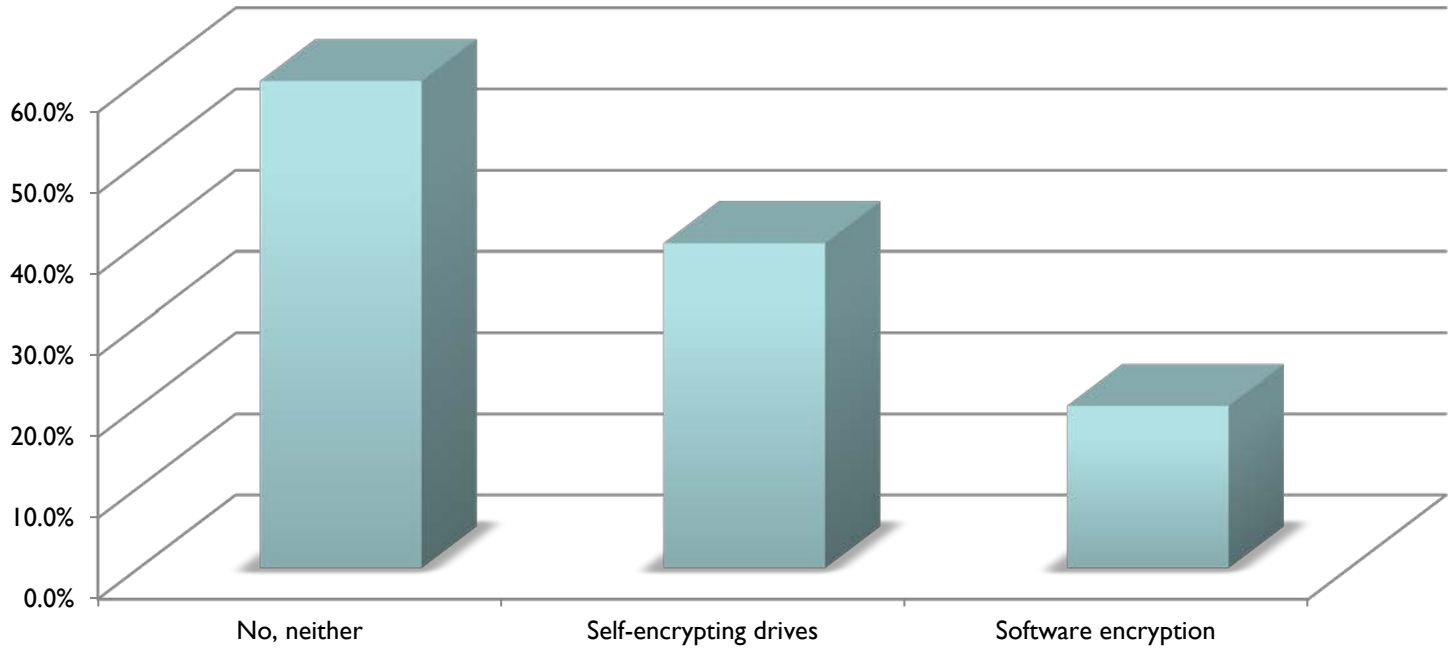
Report Results

Do you currently use SEDs in client or personal computer applications?



Report Results

Do you use self-encrypting drives or some other hardware encryption or software encryption for your stored content?



References

- NVMe over Fabrics
  - http://www.snia.org/sites/default/files/SDC15_presentations/networking/WaelNoureddine_Implementing_%20NVMe_revision.pdf
  - http://www.nvmexpress.org/wp-content/uploads/NVMe_over_Fabrics_1_0_Gold_20160605.pdf
- ISO/IEC 19790:2012
  - http://www.iso.org/iso/catalogue_detail.htm?csnumber=52906
- ISO/IEC 27040:2015
  - http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44404
- Storage Security: Encryption and Key Management
  - http://www.snia.org/sites/default/files/technical_work/SecurityTWG/SNIA-Encryption-KM-TechWhitepaper.R1.pdf
- KMIP
  - https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip
- KMIP Conformance
  - http://www.snia.org/forums/ssif/kmip

Contacts

Tom Coughlin
Coughlin Associates
tom@tomcoughlin.com
(+1) 408.202.5098
http://www.tomcoughlin.com

Walt Hubis
Hubis Technical Associates
walt@hubis.com
(+1) 303.641.8528
http://www.hubistech.com/