

Consumerization of Trusted Computing

Track: Consumerization's Impact on Infrastructure

Dr. Michael Willett
Samsung

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

© 2013 Storage Networking Industry Association. All Rights Reserved.

ABSTRACT: Consumerization of Trusted Computing

State, Federal, and international legislation mandate the use of strong security measures to protect confidential and personal information. Businesses and governments react through due diligence by implementing security best practices. In fact, being secure in their management of information provides a competitive advantage and enhances the trust that consumers of products and services have in business/government.

The modern consumer also manages confidential and personal data, as well as sensitive applications. Net: The consumer, especially in this highly interconnected world, requires equivalent security best practices. The difference is the broad range of technical expertise in the consumer population (all of us!). The security functionality must be:

- Easy to use
- Transparent
- Robust
- Inexpensive

And, be a natural part of the computing infrastructure. Enter: Trusted computing, as defined and standardized by the Trusted Computing Group (TCG). The tenets of the TCG include: robust security functions in hardware, transparency, and integration into the computing infrastructure; a perfect match with the consumer requirements.

The TCG, an industry consortium with a broad industry, government, and international membership, has developed technical specifications for a number of trusted elements. Included are specifications for integrated platform security, network client security and trust, mobile device security, and trusted storage; all key components of the consumer computing experience.

For example, the storage specifications define the concept of Self-Encrypting Drives (SED). SEDs integrate the encryption into the drive hardware electronics, encrypting all data transparently that is written to the drive; and, with no loss in drive performance. The SED protects against loss or theft, whether a laptop or a data center drive. And, both business professionals and rank-and-file consumers lose a significant number of laptops, according to the FBI. The robust protection afforded the consumer is transparent, inexpensive, and easy to use.

Combining the performance, longevity, quietness, and ruggedness of a solid-state drive (SSD) with the SED function equips the consumer with a winning combination, all integrated into the infrastructure.

The session will provide:

- Overview of the security challenges facing the consumer
- Introduction to the tenets of the Trusted Computing Group, especially the integration of security into the computing infrastructure
- Description of the TCG/SED technology, as a relevant example of trusted computing

© 2013 Storage Networking Industry Association. All Rights Reserved.

ABSTRACT: Consumerization of Trusted Computing

State, Federal, and international legislation mandate the use of strong security measures to protect confidential and personal information. Businesses and governments react through due diligence by imple… their management of information provides a competitive advantage and enhances the trust that … rnment.

The modern consumer also manages … confidential a… e consumer, especially in this highly interconnected world, requires … nical expertise in the consumer population (all of us!). The security functionality … e:

- Easy to use
- Transparent
- Robust
- Inexpensive

And, be a natural part of the computing infrastructu… d by the Trusted Computing Group (TCG). The tenets of the TCG include: robust security functio… computing infrastructure; a perfect match with the consumer requirements.

The TCG, an industry consortium with a br… and … ed technical specificati… a number of trusted elements. Included are specifications for integrated platform security, network client security and trust, mobile device security, an… storage; all key components of the consumer computing experience.

For example, the storage specifications define the c… he encryption into the drive… re electronics, encrypting all data transparently that is written to the … rotects against loss or t… er a laptop or a data center drive. And, both business professionals a… ntop… he robust protection afforded the consumer is transparent, inexpensive, a…

Combining the performance, longevity, quietness, an… on equips the consumer with a winning combination, all integrated into the infrastructure.

The session will provide:

- Overview of the security challenges fac…
- Introduction to the tenets of the Trusted … urity into the computing infrastructure
- Description of the TCG/SED technology, as a relevant example of trusted computing

Consumerization of I.T.

Easy to use
Transparent
Robust
Inexpensive

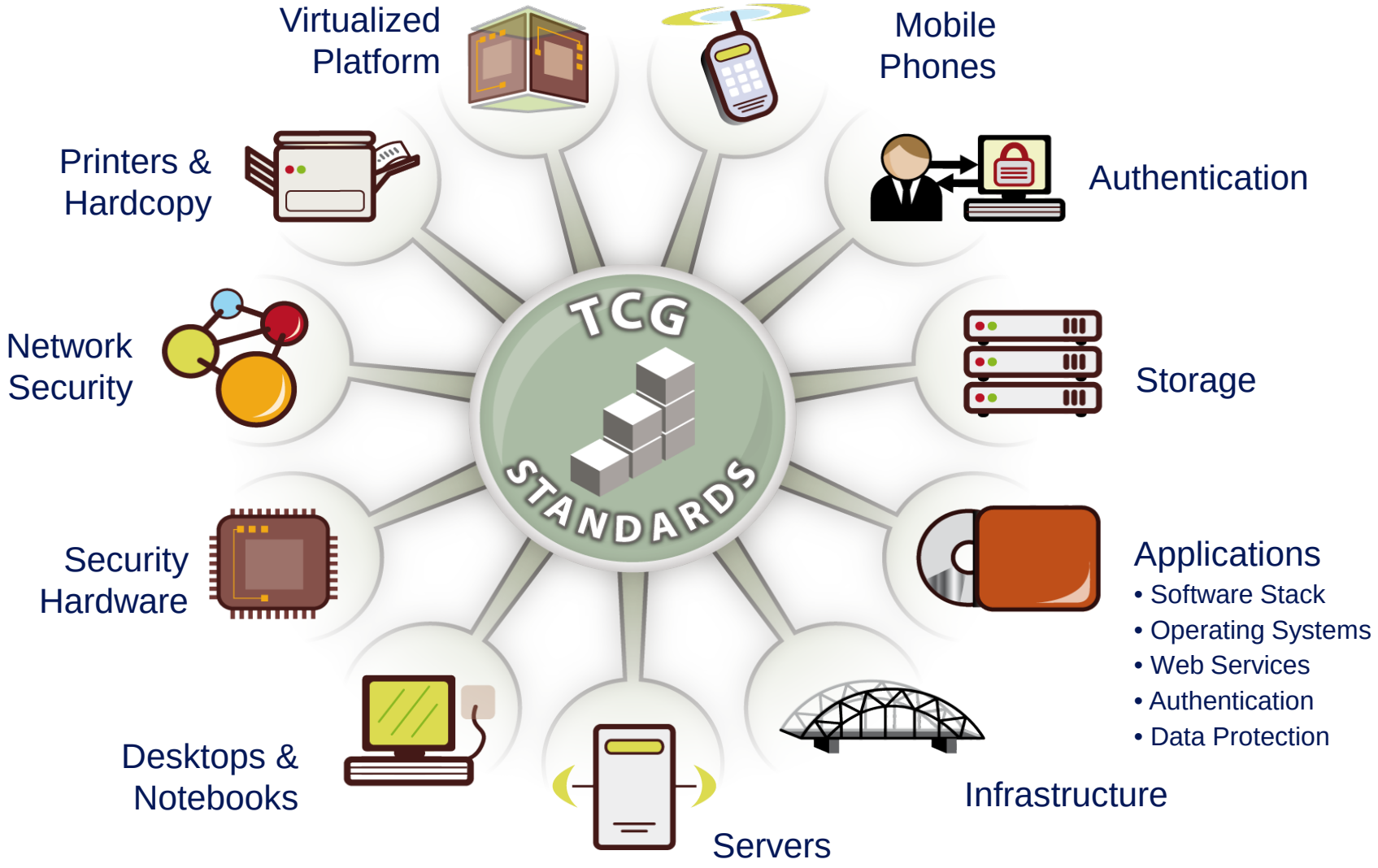
COMPLIMENTARY

Trusted Computing Group

robust security in hardware
transparency
integration into infrastructure

© 2013 Storage Networking Industry Association. All Rights Reserved.

Trusted Computing Group Standards



© 2013 Storage Networking Industry Association. All Rights Reserved.

Trust ≡ Security: Trusted Computing Concepts

- Only known machines are accessing networks, where they are recognized as authorized. Health and compliance also can be determined.
- Data at rest is encrypted on the fly and all the time with on-drive hardware security.
- A machine runs only validated code
- Only services and authorized users/machines can have a relationship
- Authentication and data protection are the priority for a successful cloud service

***Trusted Computing Group** and its specifications/standards based on hardware root of trust make this possible today*

© 2013 Storage Networking Industry Association. All Rights Reserved.

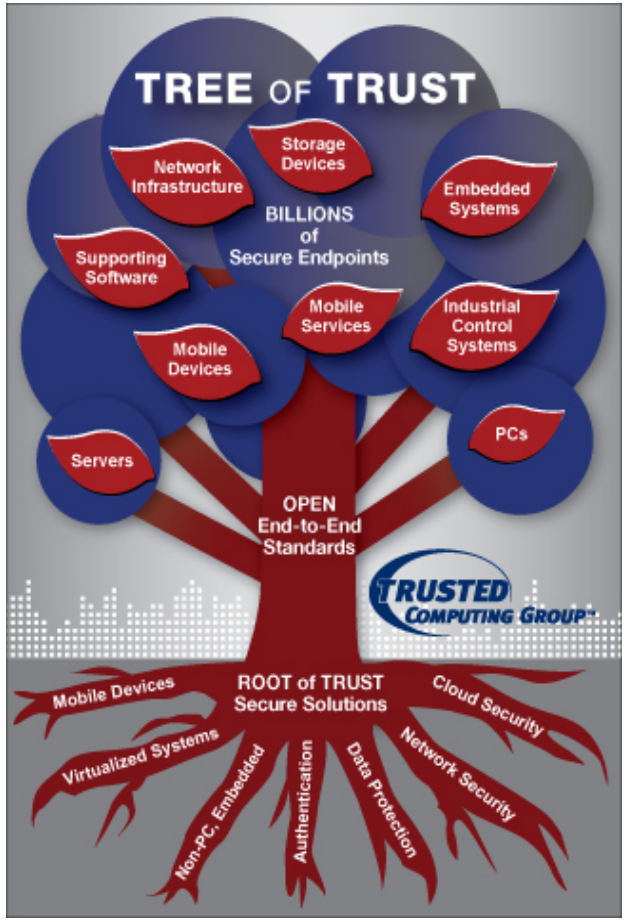
How Do Standards Benefit Security?

- Using TCG standards reduces cost
  - TPM is half the cost of a smart card, one-third the cost of a token – provides built-in authentication
  - TPMs are in every enterprise system now
- TCG standards cut deployment time
  - Already deployed on millions of products
  - Turn it on - no IT restart required
  - Plug and play with other available products such as Windows, Win Server, open source
- TCG enables multi-vendor interoperability
  - Standards-based products work with each other, offering users choice, lowering cost and fostering innovation
  - Plugfests ensure products work the same in different implementations
- International standardization and broad distribution drives adoption and membership in TCG
  - ISO/IEC has approved the TPM specification



© 2013 Storage Networking Industry Association. All Rights Reserved.

Secure Endpoints from a Trusted Foundation



The Trusted Computing Group (TCG) develops open security standards and specifications based on a root of trust enabling secure interoperable systems and networks across industries and endpoints.

- Root of trust
  - The foundation of all TCG specifications
  - Proven concepts to ensure the integrity of systems
  - Protection of data and security for networks
- Open end-to-end standards
  - A membership of the leading industry, government institutions and academic outreach
  - Membership is global and drives international standards
  - Open specifications free to developers, manufacturers and users
- TCG is a category of secure computing
  - Created billions of secure endpoints
  - Across industries and technologies

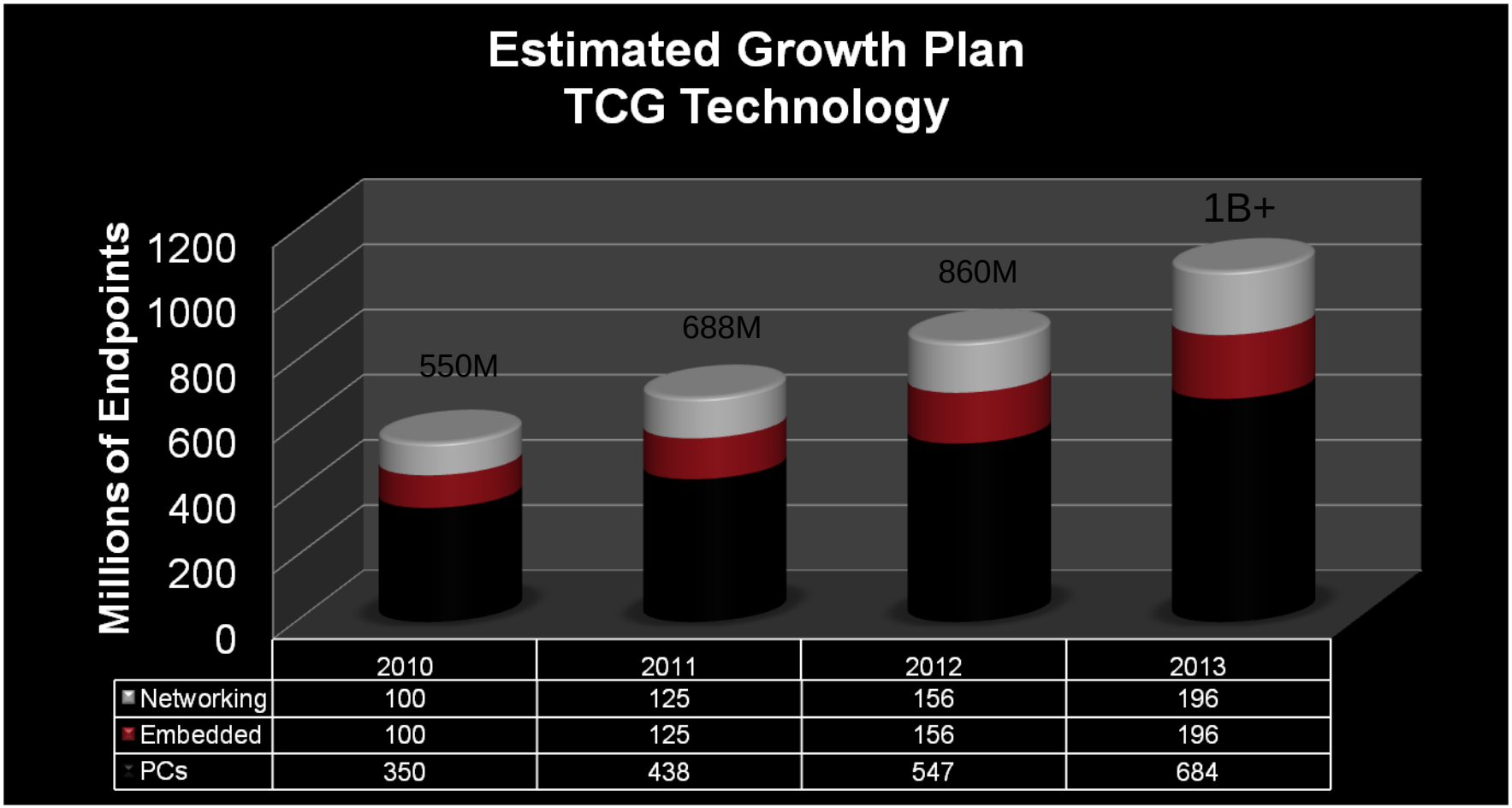
© 2013 Storage Networking Industry Association. All Rights Reserved.

Trusted Systems: Now Ubiquitous



© 2013 Storage Networking Industry Association. All Rights Reserved.

Trusted Systems Widely Available



© 2013 Storage Networking Industry Association. All Rights Reserved.

Authentication

Trusted Platform Module (TPM): Nearly every business laptop comes with an embedded security token. TPMs uniquely support both user and machine authentication in one token, ensuring only authorized users and authorized PCs are on the network.



email	Strengthen certificate-based email encryption with TPM key protection. Support for all X.509 certificate-based email encryption.
Multi-factor Authentication	Use the TPM for authentication to provide a first factor: "something you have." An additional factor can be added for security such as a PIN or password for "something you know."
VPN Access	A TPM can achieve a hardware level of security without the costs and hassles associated with deploying and managing smart cards or hardware tokens.
Wireless Access	A TPM securely can identify a user or machine and automatically integrates with the 802.1x authentication framework.

© 2013 Storage Networking Industry Association. All Rights Reserved.

Network Access and Identify

TNC = Trusted Network Connect

Guest Access	TNC specifications enable vendors to craft effective systems that enable guest access, without threat to the host network.
User Authentication	TNC supports authentication of users to further protect the network and to better manage who is using the network and what is happening.
Endpoint Integrity	TNC provides a common way to health-check clients as they attach to the network. Based on the user's own policies, these clients can be blocked from the network, quarantined, or sent to a separate network for remediation.
Clientless Endpoints	Non-PC devices such as IP phones, cameras, physical security equipment and printers connect to the network and must be assessed for threats and vulnerabilities.
Decision Making	TNC's IF-MAP specifications provide a common way for security tools to communicate, resulting in data that can be shared and used at and during the network admission processes.



© 2013 Storage Networking Industry Association. All Rights Reserved.

Mobile Security

MTM = Mobile Trusted Module

Authentication	Many tablets have TPMs and Windows 8 for embedded security. Mobile Trusted Module, MTM, offers a hardware root of trust in the device supports secure transaction, safe storage of keys and certificates and assurance of integrity.
Data protection	TCG offers standardized approach to encrypting storage devices where data is stored.
Transaction security	TCG is aligned with Mobey Forum [1] to support secure mobile financial transactions. Root of trust concept protects transactions and data.
BYOD security	TNC specifications enable identification and management of employee devices connecting to the corporate network.
Works with other mobile standards	TCG works with the Global Platform Alliance to support its Trusted Execution Environment. Aligned with Mobey Forum to support secure mobile financial transactions.



1. http://www.mobeyforum.org/ **Mobile Financial Services**

© 2013 Storage Networking Industry Association. All Rights Reserved.

Cloud Security

End-to-end security	Trusted Computing concepts allow cloud users to establish trust, exchange information about the platforms they use, assure compliance to agreed policies, and provide measurement of platform state.
Data protection	Stored data is encrypted by on-drive hardware
BYOD security	TNC architecture provides measurement of health and compliances for devices attaching to the cloud.
Multi-vendor, multi-source	Standards=interoperability and vendor choice

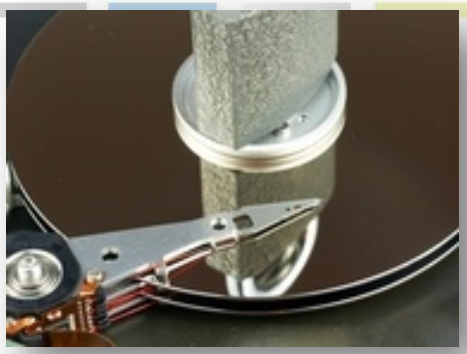


© 2013 Storage Networking Industry Association. All Rights Reserved.

Data Protection

Self-encrypting drive (SED)

solutions, based on TCG specifications, enable integrated encryption and access control within the protected hardware of the drive.



Encryption Performance	Operates at full drive speeds; scalable to large enterprises, since each drive has its own encryption engine
Stronger Security	Encryption is always on - major compliance requirement Keys for encryption are generated in the drive, never leave the drive. User authentication is performed by the drive before it will unlock, independent of the operating system
Ease-of-Use	Much easier to use than software solutions. Encryption is transparent to both users and software; comes from the factory encrypting transparently
Cost-of-Ownership	No need for complex infrastructure to manage encryption keys Main processor cycles not used for encryption No modifications to OS, applications or tools Crypto- erase provides instant repurposing / decommissioning/sanitization

© 2013 Storage Networking Industry Association. All Rights Reserved.

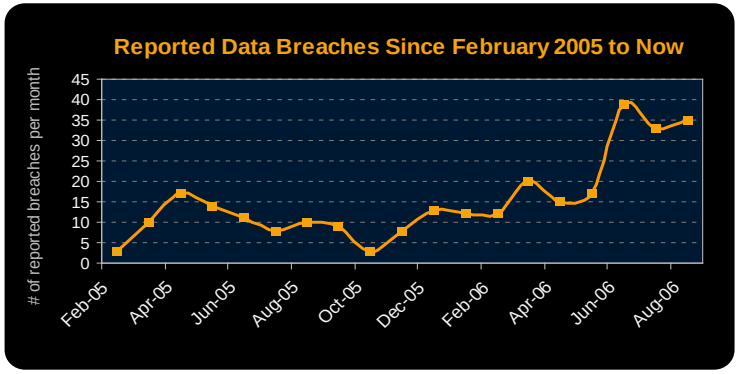
EXAMPLE: Stored Data Protection



© 2013 Storage Networking Industry Association. All Rights Reserved.

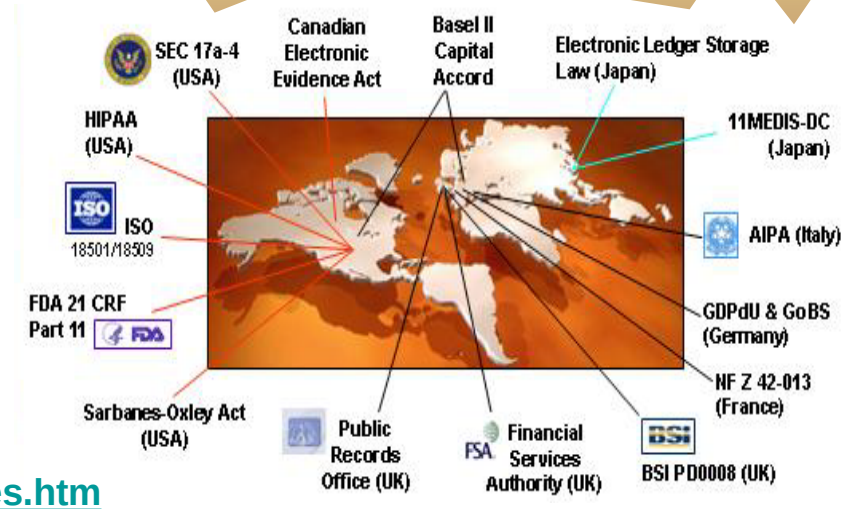
The Problem…

Since 2005, over 345,124,400 records containing sensitive personal information have been involved in security breaches



In 2008, the average cost of a data breach was $6.65 million per affected corporation ($202 per record)

$6.65 Million Per Incident



http://www.privacyrights.org/ar/ChronDataBreaches.htm

© 2013 Storage Networking Industry Association. All Rights Reserved.

The Problem…

Since 2005, over 345,124,400 records containing sensitive personal information have been involved in security breaches

Legal

Financial

Reputation

…a breach was $6.65 million per affected corporation ($202 per record)

…r Incident





http://www.privacyrights.org/ar/ChronDataBreaches.htm

© 2013 Storage Networking Industry Association. All Rights Reserved.

Breach Notification Legislation

Example: California

… any agency that owns or licenses computerized data that includes personal information shall **disclose any breach** of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose **unencrypted** personal information was, or is reasonably believed to have been, acquired by an unauthorized person…"

Encryption "safe harbor"

© 2013 Storage Networking Industry Association. All Rights Reserved.

Why Encrypt Data-At-Rest?

SNIA Education

Threat scenario: stored data leaves the owner's control – lost, stolen, re-purposed, repaired, end-of-life, …

- Compliance
  - **48+ U.S. states have data privacy laws with encryption "safe harbors", which exempt encrypted data from breach notification[1]**

- EU: Replace Data Protection Directive 95/46/EC (27 countries)

  requires breach notification [3]

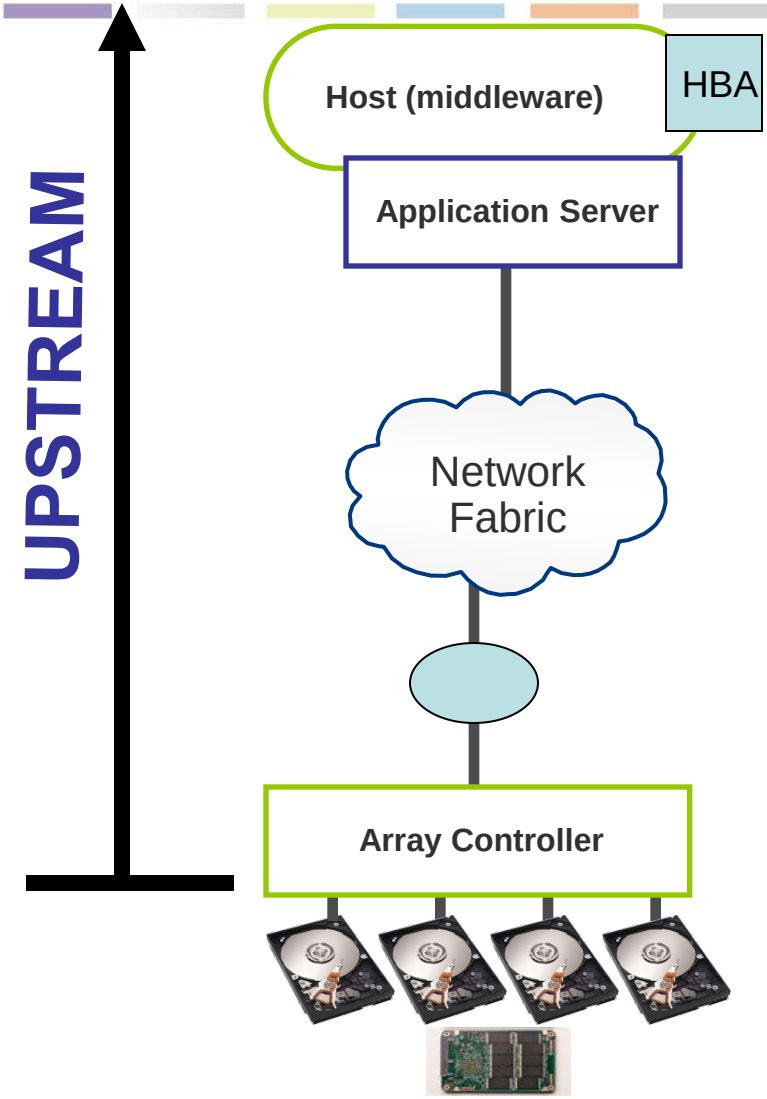
- Exposure of data loss is expensive ($6.65 Million on average per incident[2])

- Obsolete, Failed, Stolen, Misplaced…
  - **Nearly ALL drives leave the security of the data center**
  - **The vast majority of retired drives are still readable**

1. http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx
2. Ponemon Institute, Annual US Cost of Data Breach Study – www.ponemon.org
3. https://www.eiseverywhere.com/file_uploads/4982c29aa16310269434b49b0ac62eed_EricHibbard_Data-Breach-Encryption-Safe-Harbor_Final.pdf

© 2013 Storage Networking Industry Association. All Rights Reserved.

Encryption can be done in a number of places…



Host middleware

Host HBA (h/w adapter)

Application

Switch

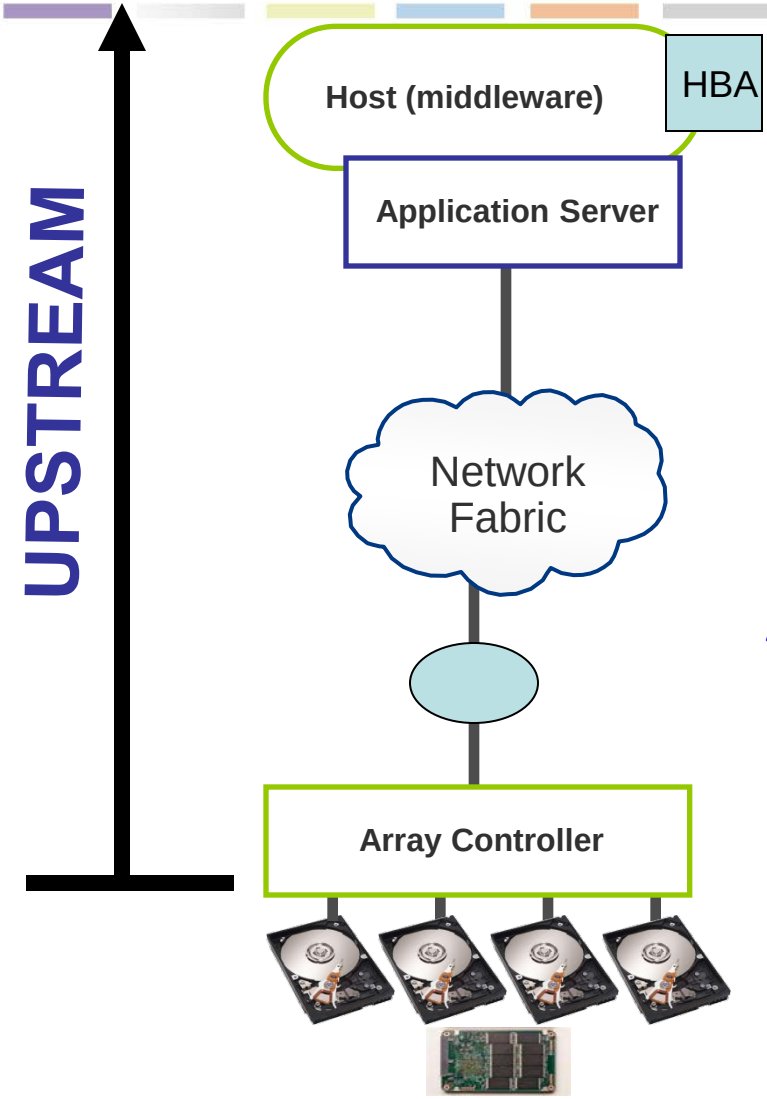
“Bump in the wire” or proxy appliance

Array controller

Drive (HDD, SSD)

© 2013 Storage Networking Industry Association. All Rights Reserved.

Encryption can be done in “layers”…



Host middleware

Host HBA (h/w adapter)

Application

LAYERED APPROACH

Switch

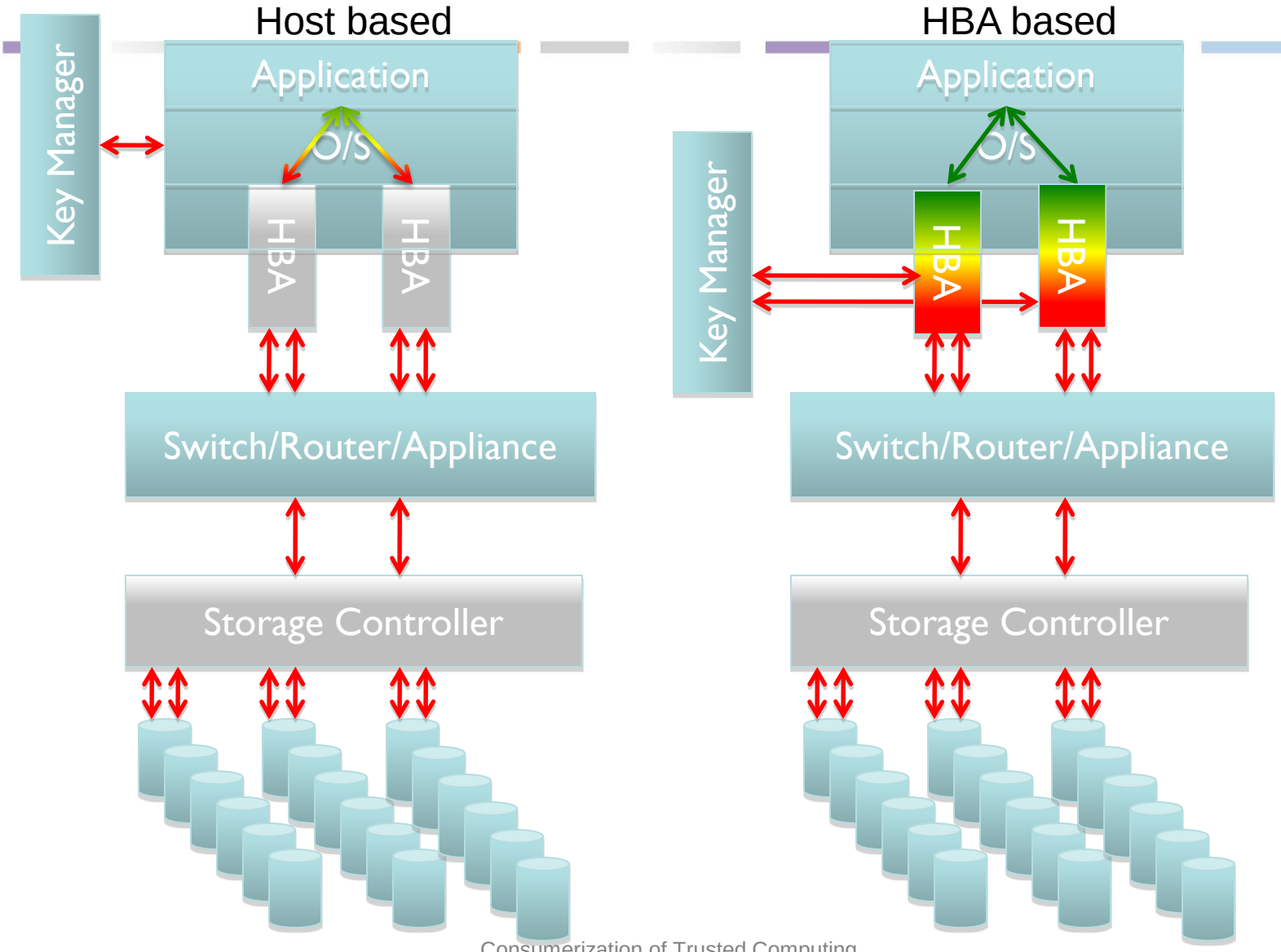
“Bump in the wire” or proxy appliance

Array controller

Drive (HDD, SSD)

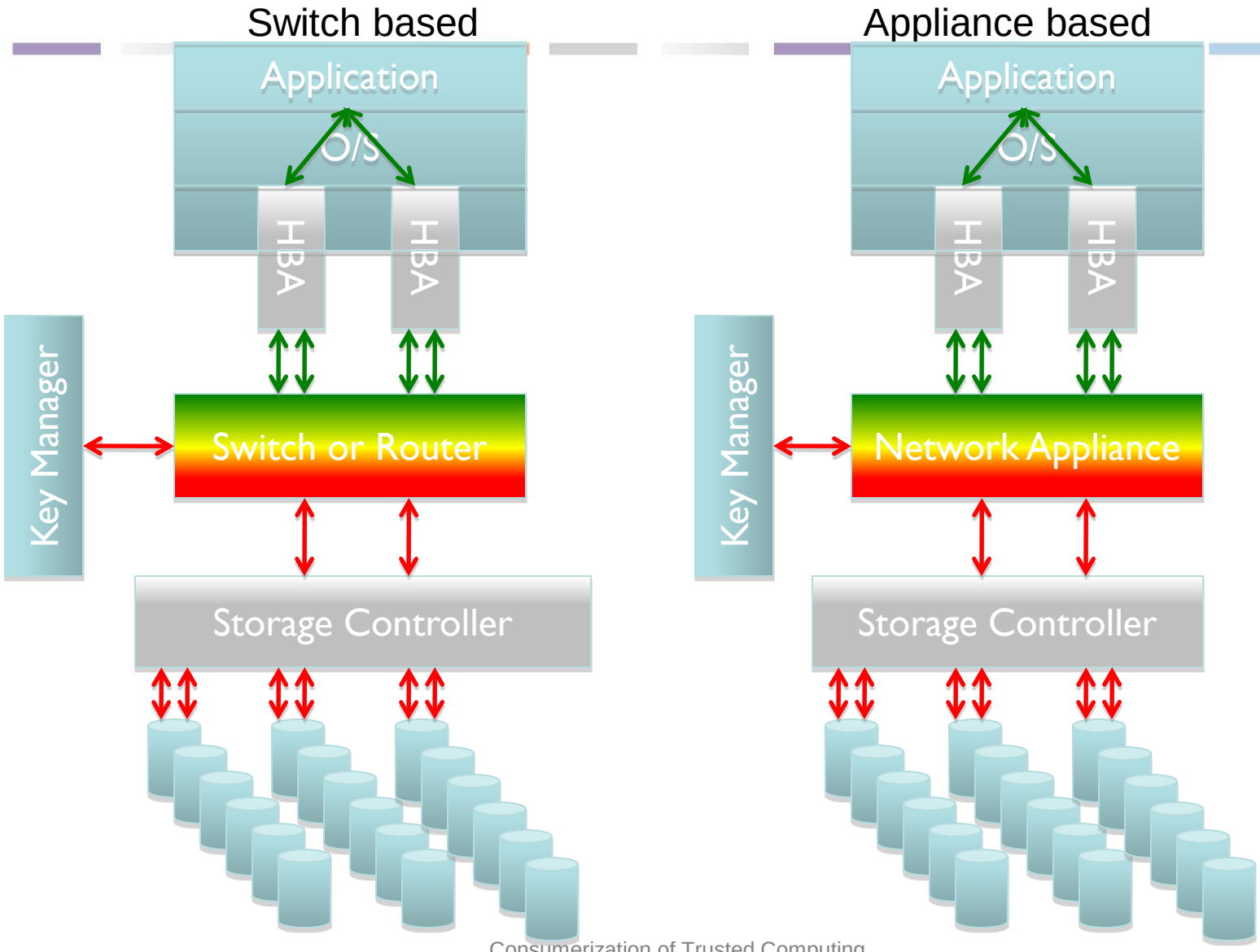
© 2013 Storage Networking Industry Association. All Rights Reserved.

Host and HBA Based Encryption



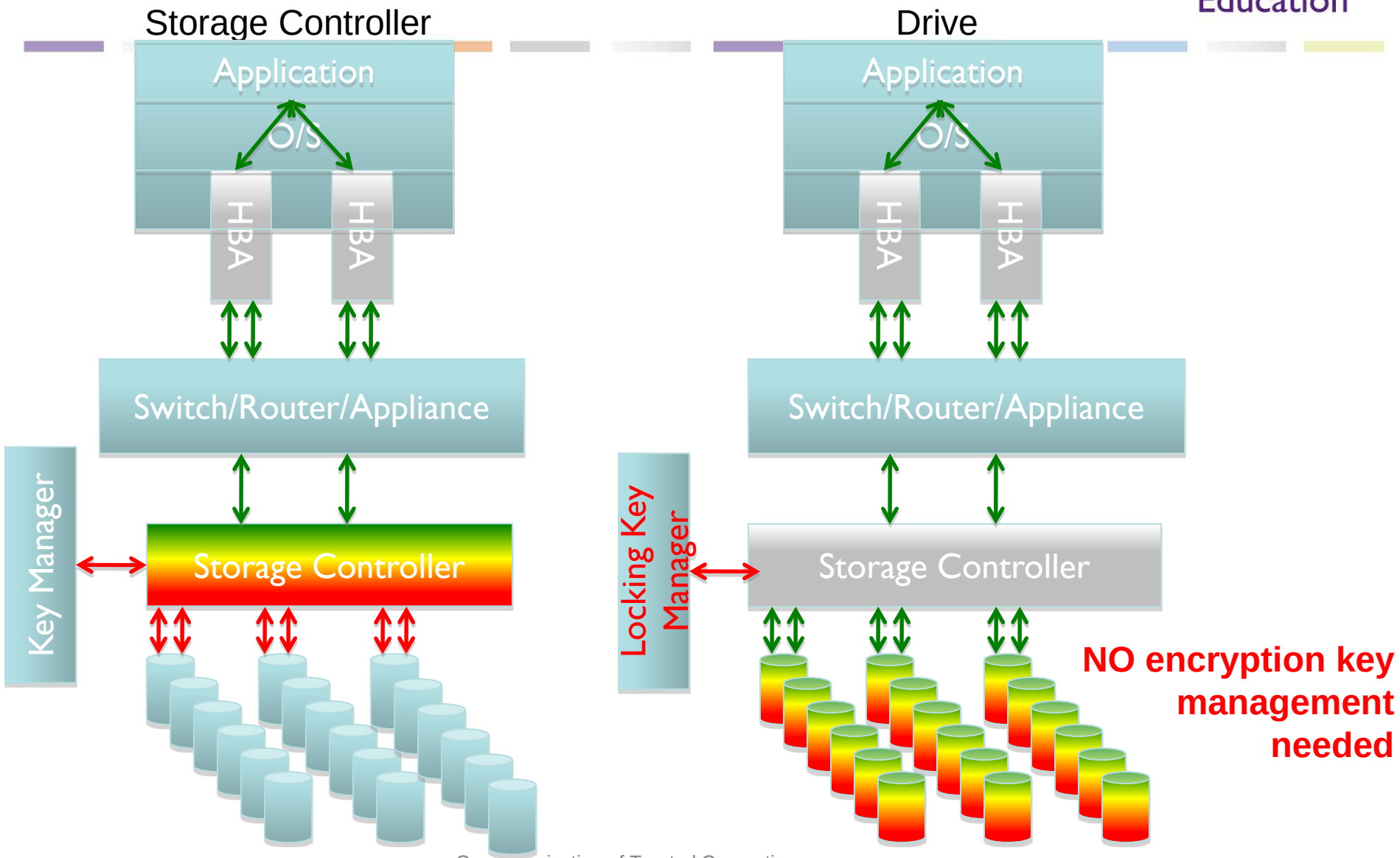
© 2013 Storage Networking Industry Association. All Rights Reserved.

Switch or Appliance Based Encryption



© 2013 Storage Networking Industry Association. All Rights Reserved.

Storage Controller or Drive-Based Encryption



© 2013 Storage Networking Industry Association. All Rights Reserved.

SNIA Nine-Step Checklist

SNIA Education

Encryption of Data At-Rest
Step-by-step Checklist
Version 2.0
9 September 2009

(available @ http://www.snia.org/forums/ssif/knowledge_center/white_papers/)

© 2013 Storage Networking Industry Association. All Rights Reserved.

The Steps

1. Understand Drivers
2. Classify Data Assets
3. Inventory Data Assets
4. Perform Data Flow Analysis
5. Choose Points-of-Encryption
6. Design Encryption Solution
7. Begin Data Re-Alignment
8. Implement Solution
9. Activate encryption

© 2013 Storage Networking Industry Association. All Rights Reserved.

The Steps (using SEDs)

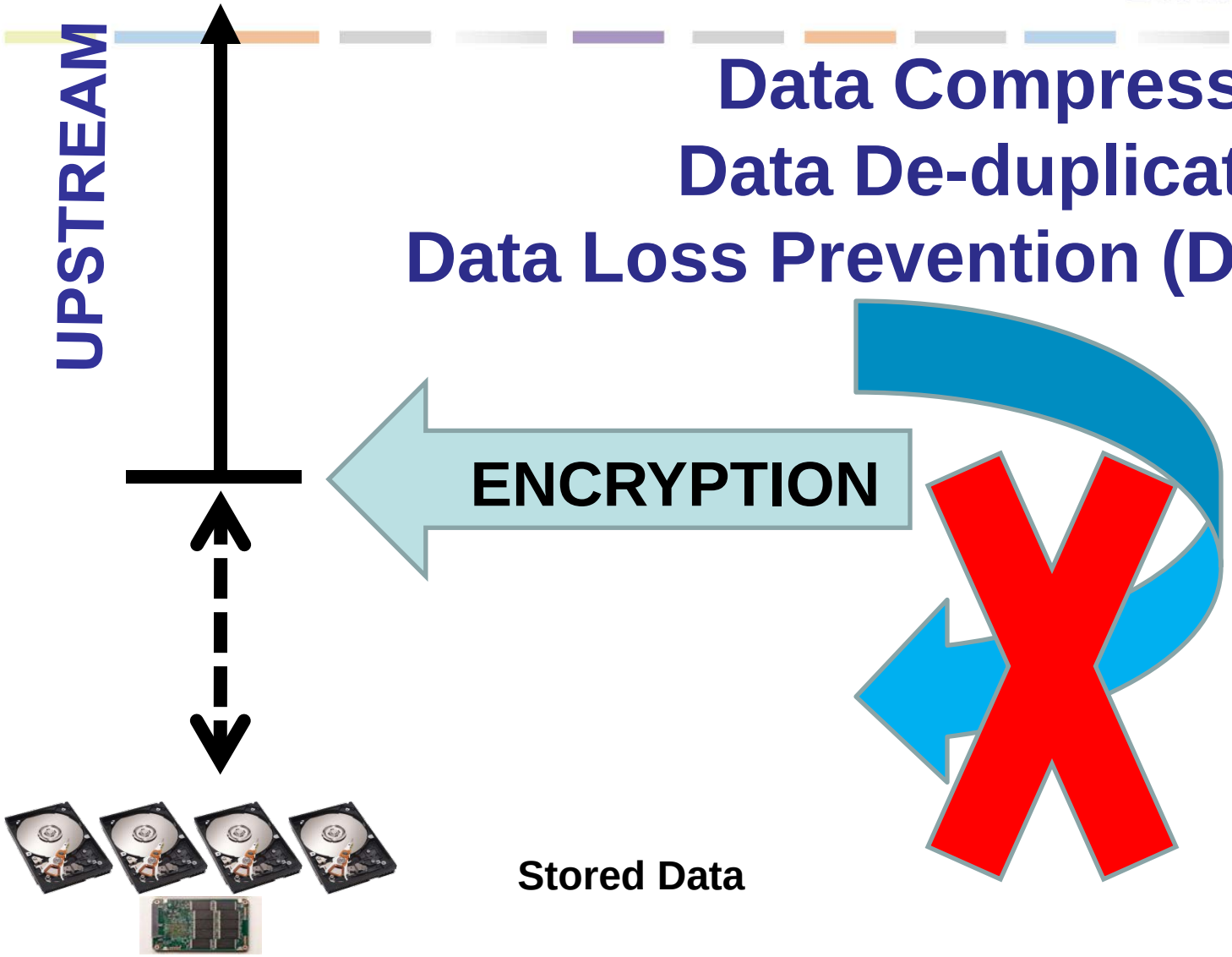
1. Understand Drivers: **breach laws**
2. ~~Classify Data Assets~~
3. ~~Inventory Data Assets~~
4. ~~Perform Data Flow Analysis~~
5. Choose Points-of-Encryption: **drives**
6. Design Encryption Solution: **management**
7. ~~Begin Data Re-Alignment~~
8. Implement Solution: **SED phase-in**
9. Activate encryption: **automatic**

Greatly Simplified Using SEDs

- Data classification and asset inventory not required to support SEDs
- Higher layer encryption may additionally be mandated by regulations

© 2013 Storage Networking Industry Association. All Rights Reserved.

Encryption upstream can affect other processes



Data Compression
Data De-duplication
Data Loss Prevention (DLP)

© 2013 Storage Networking Industry Association. All Rights Reserved.

Trusted Storage Standardization





© 2013 Storage Networking Industry Association. All Rights Reserved.

SED Superiority

- Simplified Management
- Robust Security
- Compliance "Safe Harbor"
- Cuts Disposal Costs
- Scalable
- Interoperable
- Integrated
- Transparent

"Many organizations are considering **drive-level security for its simplicity** in helping secure sensitive data through the hardware lifecycle from initial setup, to upgrade transitions and disposal"

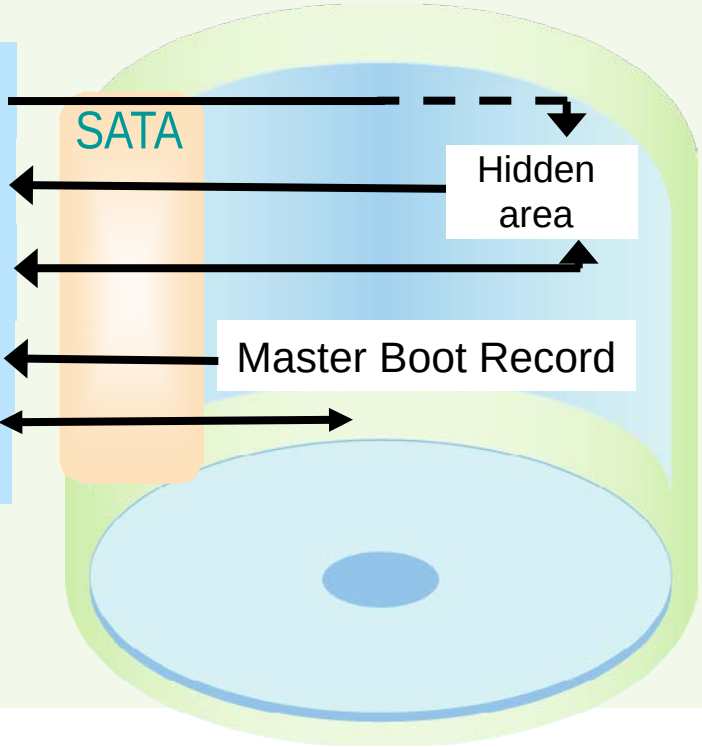
Eric Ouellet
Research Vice President
Gartner

© 2013 Storage Networking Industry Association. All Rights Reserved.

Client Security: Pre-Boot Authentication

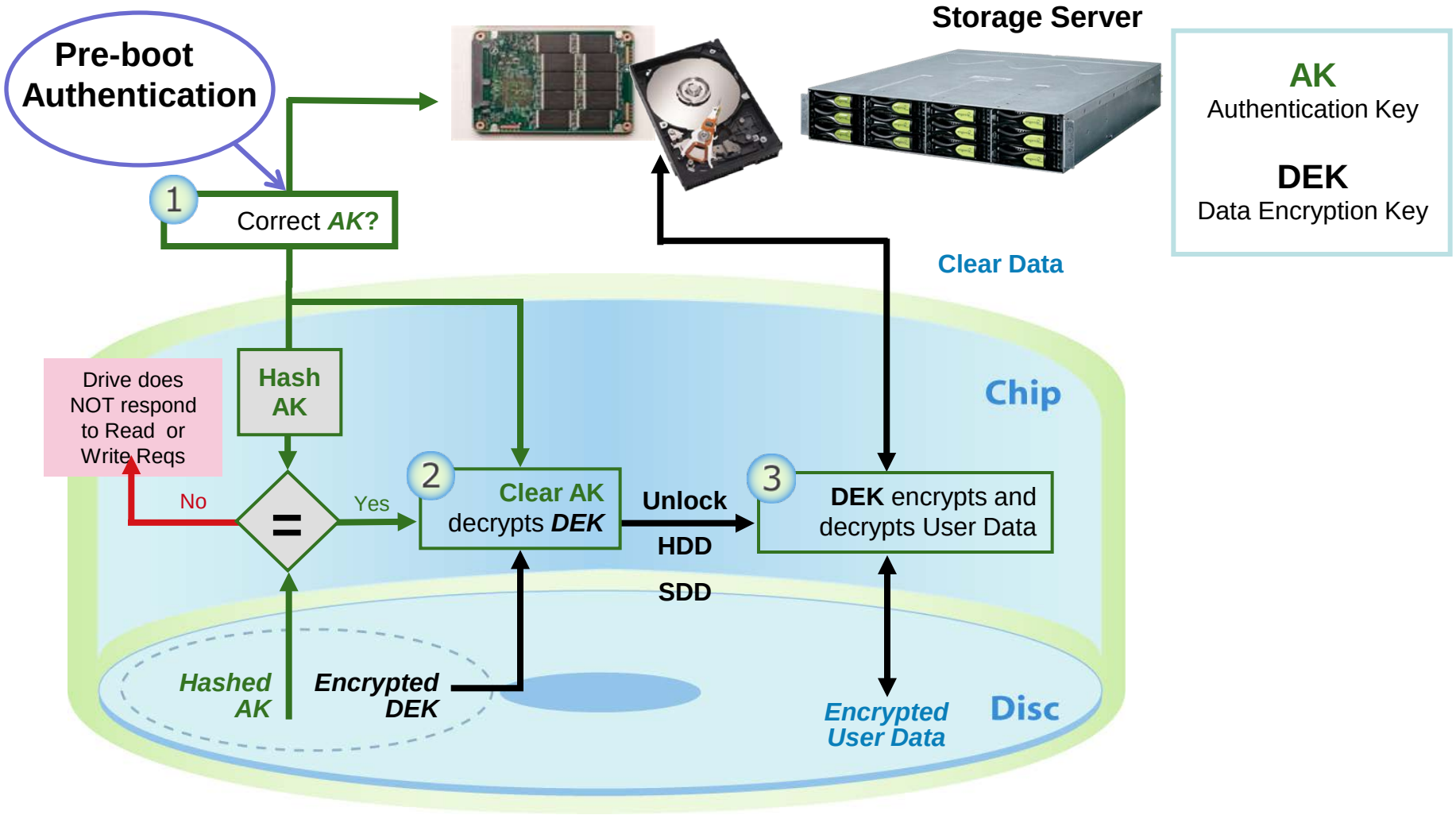
- **Transparency: Master boot record and OS are unmodified**
- **Protected from malicious software: Authentication occurs before OS (and any malicious software) is loaded**
- **The master boot record can't be corrupted: The entire drive, including the master boot record, is encrypted**

1. BIOS attempts MBR read; drive redirects to pre-boot area
2. Drive loads pre-boot OS
3. User enters authentication credentials for drive to verify
4. If authentication successful, drive loads original MBR
5. Normal operation commences



© 2013 Storage Networking Industry Association. All Rights Reserved.

Authentication in the Drive



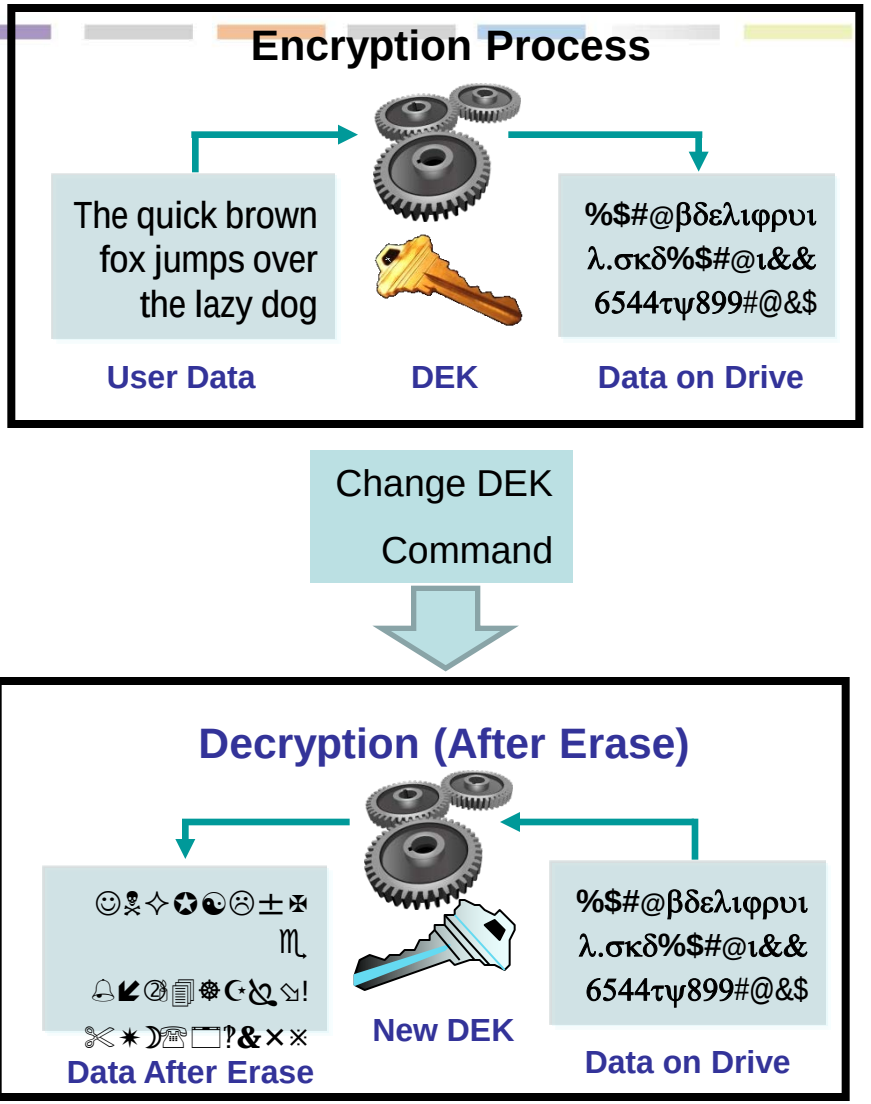
© 2013 Storage Networking Industry Association. All Rights Reserved.

Crypto Erase

SNIA Education

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

- Revision 1 of U.S. NIST SP800-88: **Guidelines for Media Sanitization** under way to support Crypto Erase

http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf

© 2013 Storage Networking Industry Association. All Rights Reserved.

‘Hurdles’ to Implementing Encryption…

Key management / data loss	• Tracking and managing encryption keys • Tracking and managing authentication keys (passwords for unlocking drives)
Complexity	• Data classification • Impact on OS, applications, databases • Interoperability
Performance	• Performance degradation; scalability
Cost	• Initial acquisition costs • Deployment costs

© 2013 Storage Networking Industry Association. All Rights Reserved.

No Performance Degradation



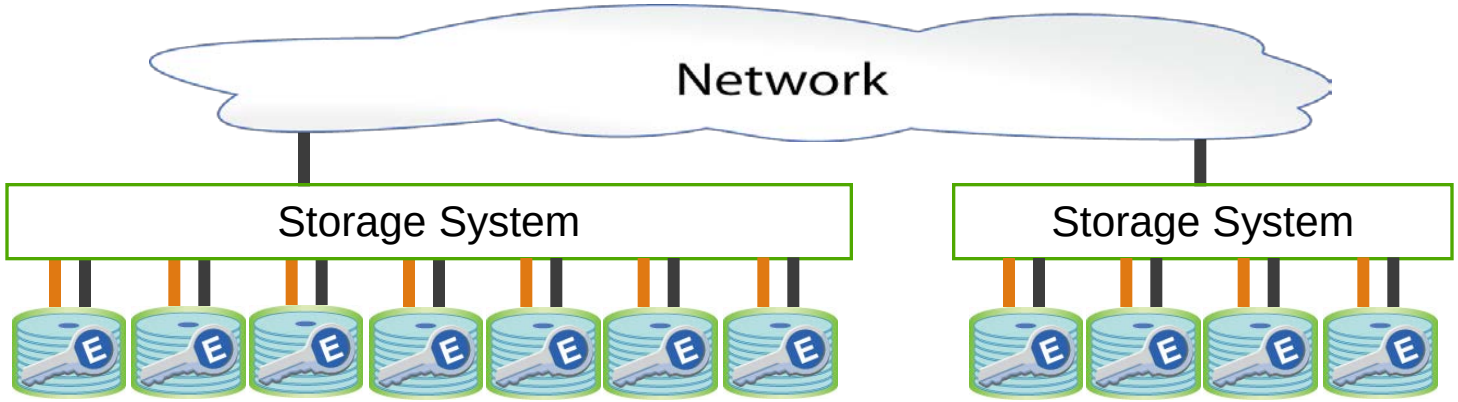
Encryption engine speed

Matches

Port's max speed

The encryption engine is in the drive electronics

Scales Linearly, Automatically



All data will be encrypted, with no performance degradation

© 2013 Storage Networking Industry Association. All Rights Reserved.

IT Retires Drives Constantly



- All Drives are Eventually Retired
  - End of Life
  - Returned for Expired Lease
  - Returned for Repair / Warranty
  - Repurposed
- 50,000 drives leave data centers daily
- Exposure of data is expensive - $6.65 million on average
- 90% of retired drives are still readable

(IBM study[1])

Needed: A simple, efficient, secure way to make retired drive data unreadable



1: http://www.redbooks.ibm.com/redpapers/pdfs/redp4529.pdf

© 2013 Storage Networking Industry Association. All Rights Reserved.

How the Drive Retirement Process Works



Retire Drive

- Replace
- Repair
- Repurpose

Remove ALL drives

Send even "dead" drives through

Queue in Secure Area

Transport Offsite

Queue in secure area

Retirement Options



Overwriting takes days and there is no notification of completion from drive



Hard to ensure degauss strength matched drive type



Shredding is environmentally hazardous



Not always as secure as shredding, but more fun

SECURE?

People make mistakes

"Because of the volume of information we handle and **the fact people are involved, we have occasionally made mistakes.**"

IRON MOUNTAIN

which lost a tape with 150,000 Social Security numbers stored at an Iron Mountain warehouse, October 2007[1]

99% of Shuttle Columbia's hard drive data recovered from crash site

Data recovery specialists at Kroll Ontrack Inc. retrieved 99% of the information stored on the charred Seagate hard drive's platters over a two day period.

- May 7, 2008 (Computerworld)

1. http://www.usatoday.com/tech/news/computersecurity/2008-01-18-penney-data-breach_

© 2013 Storage Networking Industry Association. All Rights Reserved.

How the Drive Retirement Process Works

Retirement Options



Retire Drive

-
- Re

Overwriting takes
ere is no
cation of
om drive

o ensure
strength
rive type

g is
ntally
dous

ays as
dding,
re fun

S E C U R E ?

Drive Retirement is:

Expensive

Time-consuming

Error-prone

IRON MOUNTAIN

which lost a tape with 150,000 Social Security numbers stored at an Iron Mountain warehouse, October 2007[1]

nbia's hard drive data recovered from crash site

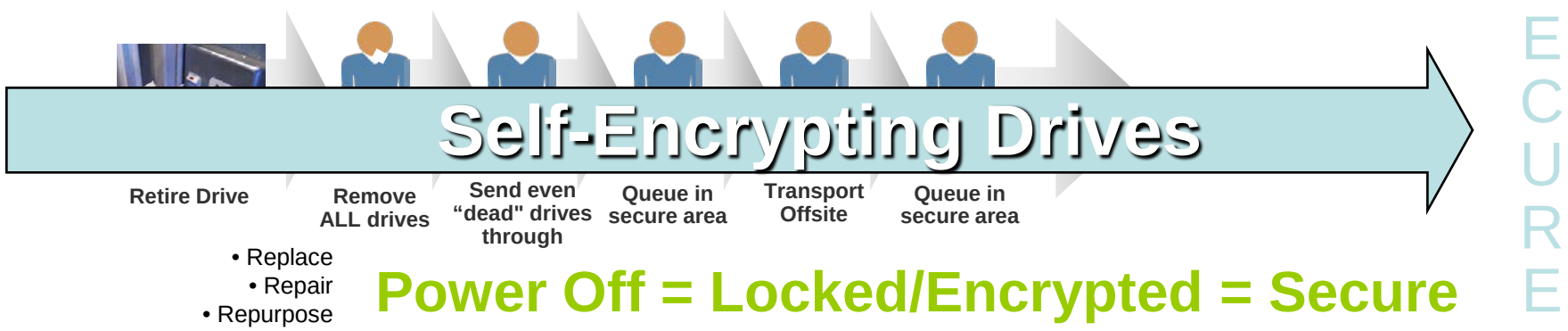
Data recovery specialists at Kroll Ontrack Inc. retrieved 99% of the information stored on the charred Seagate hard drive's platters over a two day period.

- May 7, 2008 (Computerworld)

1. http://www.usatoday.com/tech/news/computersecurity/2008-01-18-penney-data-breach_

© 2013 Storage Networking Industry Association. All Rights Reserved.

Drive Retirement: Self-Encryption



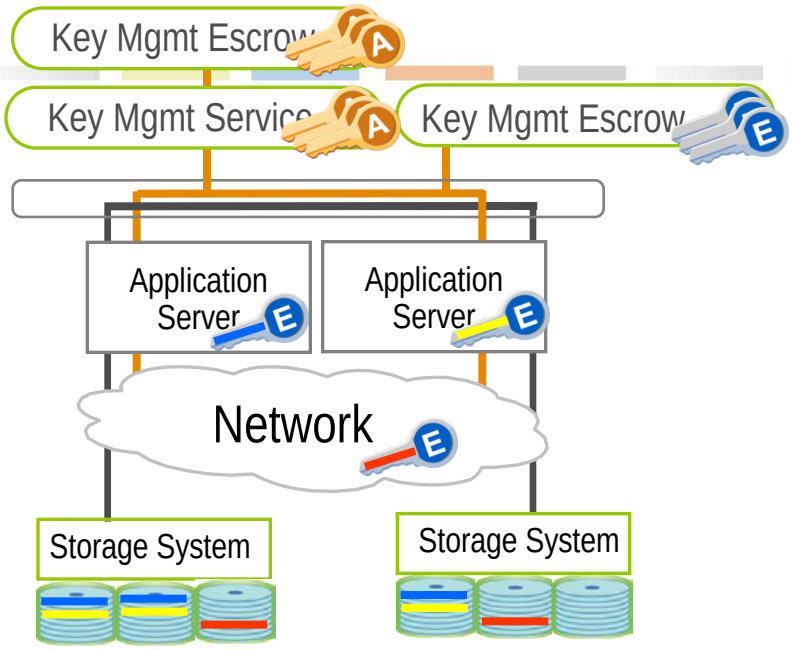
Power Off = Locked/Encrypted = Secure

Added "insurance": Crypto Erase

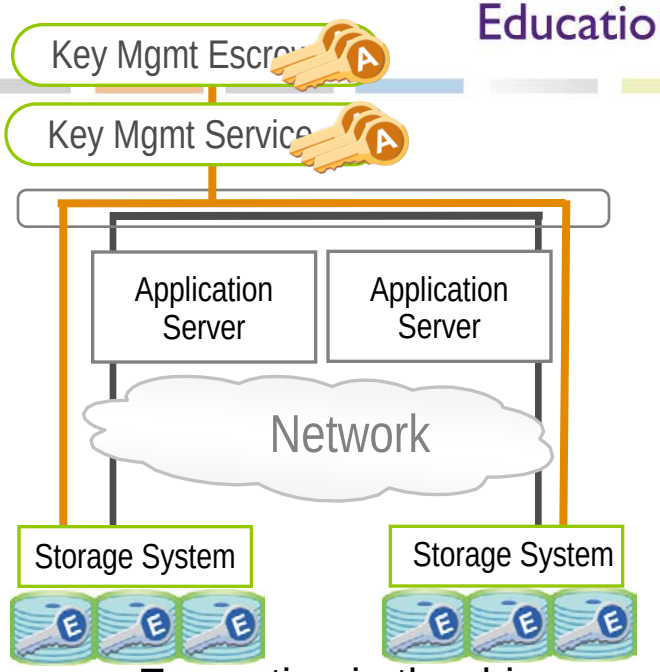
- Reduces IT operating expense
  - Eliminates the need to overwrite or destroy drive
  - Secures warranty and expired lease returns
  - Enables drives to be repurposed securely
- Provides safe harbor for most data privacy laws

© 2013 Storage Networking Industry Association. All Rights Reserved.

Key Management Simplification



Encrypting outside the drive



Encrypting in the drive

Encryption key never leaves the drive. No need to track or manage …
BUT, YOU STILL MANAGE THE AUTHENTICATION KEYS (drive locking),
to protect against loss or theft (for just crypto erase, no authentication key needed)

- **To recover data from a drive:**
  - ***Only need the Authentication Key and the drive***
  - Don't need to escrow the encryption key to maintain data recoverability
  - Don't need to track encryption key storage separate from data storage
  - Don't need to be concerned with interoperability of encryption key storage and data

© 2013 Storage Networking Industry Association. All Rights Reserved.

Hardware-Based Self-Encryption versus 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 cost:** 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

ISSUE: Hardware acquisition (part of normal replacement cycle)

© 2013 Storage Networking Industry Association. All Rights Reserved.

Performance Comparisons: HDD and SSD, software versus SED

MB/Sec	HDD: no encryption	HDD: S/W encryption	HDD: SED	SSD: no encryption	SSD: S/W encryption	SDD: SED
Startup	7.90	6.97	7.99	82.50	47.90	95.33
App Loading	7.03	5.77	5.71	48.33	30.77	60.37
Modest size file test	6.13	5.00	5.28	41.13	26.77	50.40
Large Scale Data Read	84.67	52.88	82.75	178.00	70.23	169.33
Large Scale Data Write	79.60	49.50	50.31	170.80	63.60	164.50

http://www.trustedstrategies.com/

© 2013 Storage Networking Industry Association. All Rights Reserved.

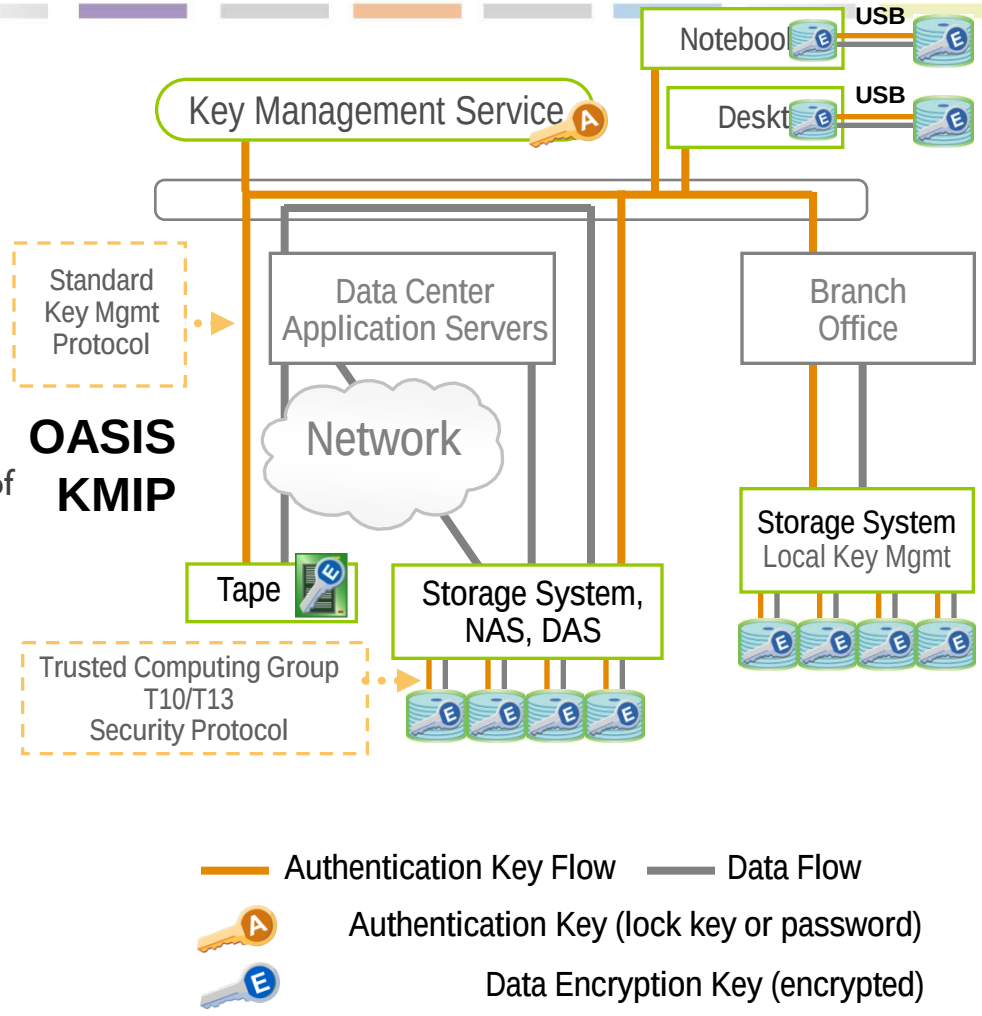
Addressing the Hurdles…

Simplifies key management to prevent data loss	✓ Encryption key does not leave the drive; it does not need to be escrowed, tracked, or managed
Simplifies Planning and Management	✓ Standards-based for optimal manageability and interoperability ✓ Transparent to application developers and database administrators. No change to OS, applications, databases ✓ Data classification not needed to maintain performance
Solves Performance	✓ No performance degradation ✓ Automatically scales linearly ✓ Can change keys without re-encrypting data
Reduces Cost	✓ Standards enables competition and drive cost down ✓ Compression and de-duplication maintained ✓ Simplifies decommissioning and preserves hardware value for returns, repurposing

© 2013 Storage Networking Industry Association. All Rights Reserved.

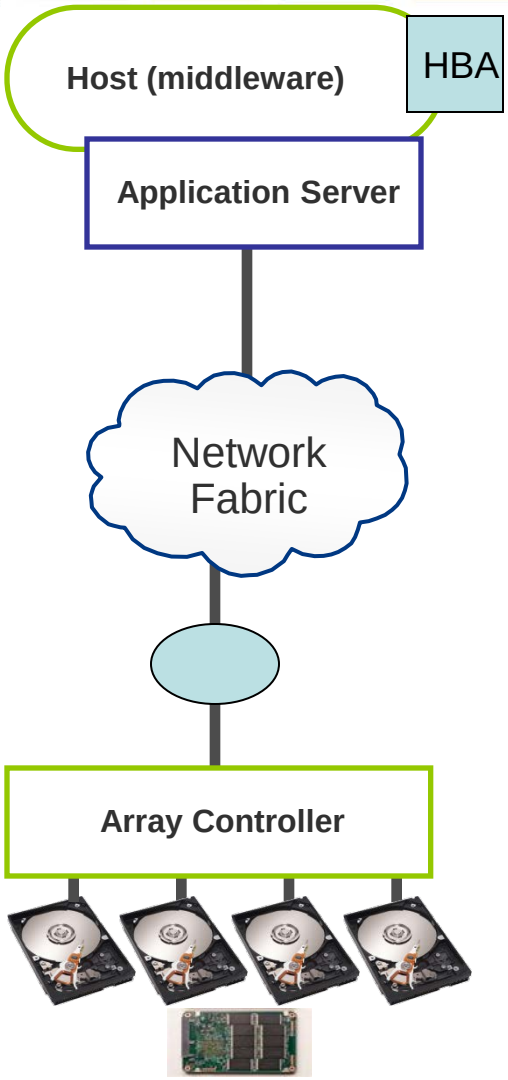
The Future: Self-Encryption Everywhere

- **Encryption everywhere!**
  - Data center/branch office to the USB drive
- **Standards-based**
  - Multiple vendors; interoperability
- **Unified key management**
  - Authentication key management handles all forms of storage
- **Simplified key management**
  - Encryption keys never leave the drive. No need to track or manage.
- **Transparent**
  - Transparent to OS, applications, application developers, databases, database administrators
- **Automatic performance scaling**
  - Granular data classification not needed



© 2013 Storage Networking Industry Association. All Rights Reserved.

SUMMARY: Layered Encryption



UPSTREAM

(clear data)

(encrypted data)

DOWNSTREAM

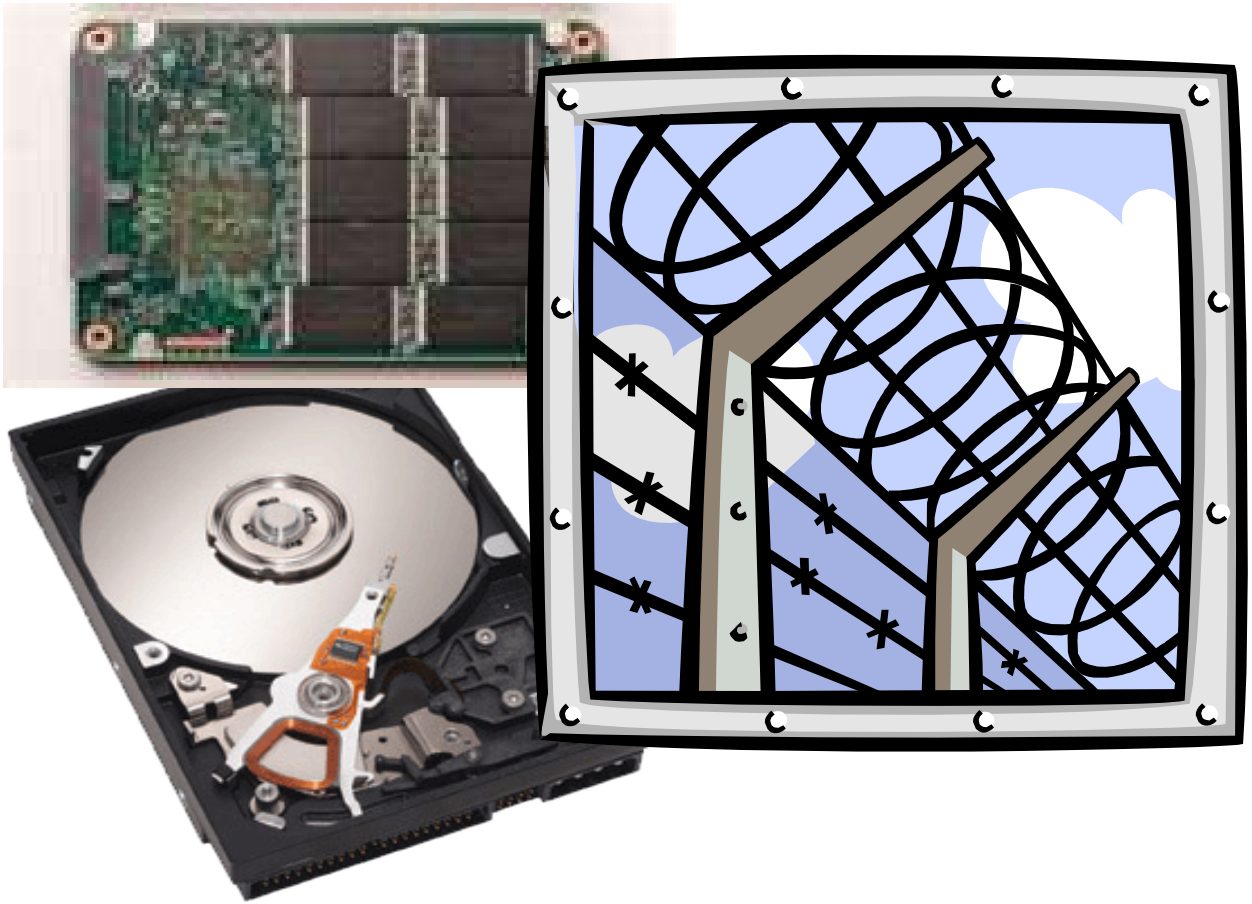
ENCRYPTION

- Higher-level encryption
- Data context awareness
- Specific legislation requirements
- Encryption-to-storage protection

- Less data context awareness
- Encryption closer to storage
- Self-encrypting drives:
  - Encrypt everything!
  - Transparently

© 2013 Storage Networking Industry Association. All Rights Reserved.

Thank You!



© 2013 Storage Networking Industry Association. All Rights Reserved.

SNIA Security: Get Involved!

- SNIA Security Technical Work Group (TWG)
  - Focus: Requirements, architectures, interfaces, practices, technology, educational materials, and terminology for storage networking.
  - http://www.snia.org/tech_activities/workgroups
- Storage Security Industry Forum (SSIF)
  - Focus: Marketing collateral, educational materials, customer needs, whitepapers including the BCPs & Encryption of Data At-Rest (a Step-by-Step Checklist)
  - http://www.snia.org/forums/ssif

© 2013 Storage Networking Industry Association. All Rights Reserved.

Attribution & Feedback

The SNIA Education Committee thanks the following individuals for their contributions to this Tutorial.

Authorship History

Dr. Michael Willett

Updates:

Trusted Computing Group

Additional Contributors

Gianna DaGiau
Joseph White
Chris Winter
Eric Hibbard
Anne Price
Brian Berger

Please send any questions or comments regarding this SNIA Tutorial to ***tracktutorials@snia.org***

© 2013 Storage Networking Industry Association. All Rights Reserved.