

Storage Security – Do You Know Where Your Data Is?

Presented by:

Eric A. Hibbard, CISSP, CISA, ISSAP, ISSMP, ISSEP
Hitachi Data Systems

Abstract

As new regulatory and legal requirements surrounding data “indiscretions” continue to emerge and the penalties become more severe, many organizations are exploring storage security options like encryption to better protect their data. Those who have ventured into this space quickly realize that there is no “panacea” that will make the problems go completely away. However, with careful planning and judicious use of the right technologies, organizations can eliminate many of their exposures.

This session focuses on ways to protect data by using security within the storage ecosystem as well as making it an important element of a defense-in-depth strategy. Best practices along with factors to consider are presented for protecting storage management, data in-flight, and data at-rest within contemporary storage environments.

The Storage Security Dilemma

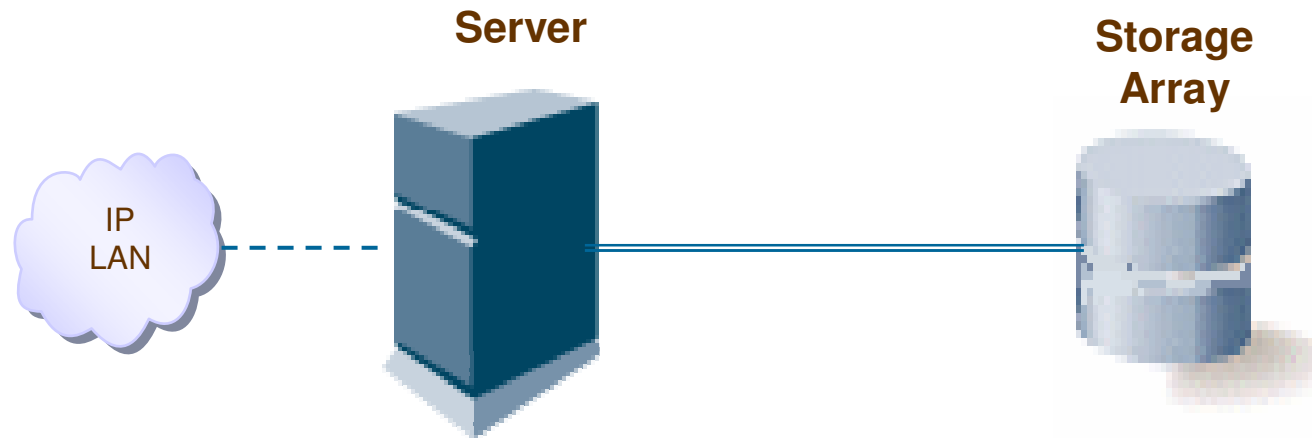
- ✦ **Organizational IT governance rarely extends to storage ecosystems**
- ✦ **Risk is rarely factored into storage ecosystem decisions**
- ✦ **Storage ecosystems have emerged in isolation with a focus on data availability and resiliency**
- ✦ **Data traceability is challenging and rarely done**
- ✦ **Auditors and security professionals frequently treat storage ecosystems as nothing more than direct-attached storage**

Why Does this Matter?

- ✦ **Organizations live and die based on the availability and integrity of their data**
- ✦ **Mishandling of sensitive data can result in severe consequences**
- ✦ **Organized crime has discovered that cyber crime is more profitable (and safer) than drug trafficking**
- ✦ **Data is no longer safely tucked away behind servers; it may be readily available**

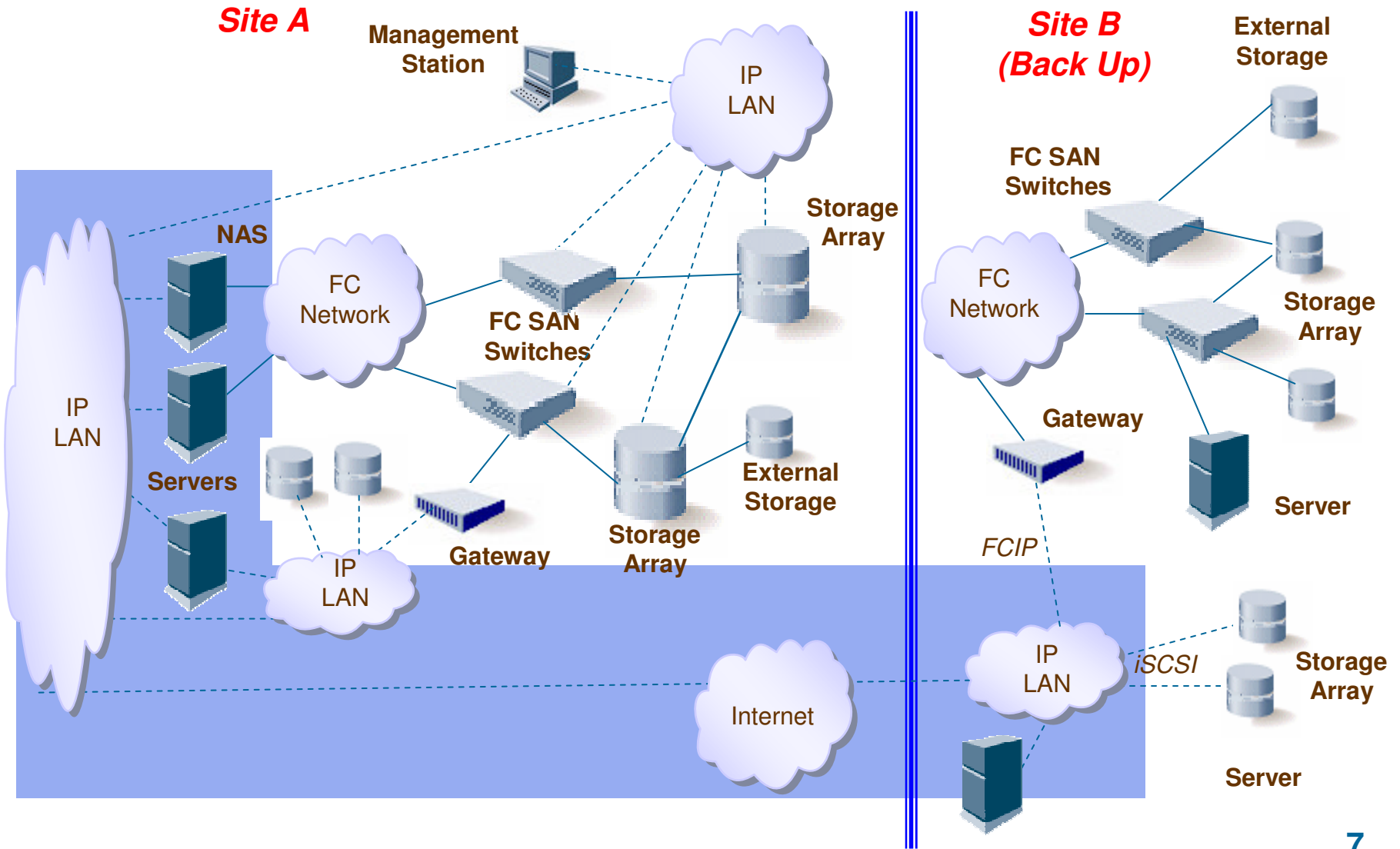
A Quick Look at Storage Ecosystems

The Not-So-Modern Storage Ecosystem (a.k.a., direct-attached storage)



Secure the server and you secure the storage.

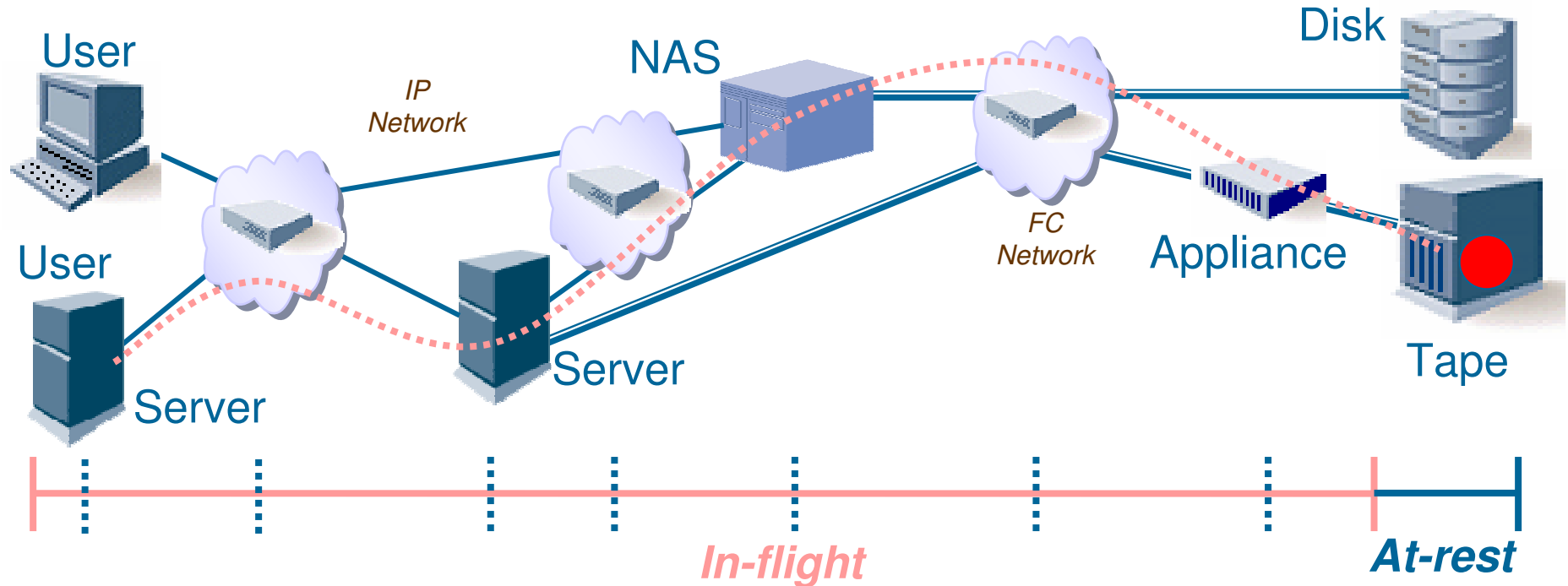
A Modern Storage Ecosystem



Storage Ecosystem – Common Elements

- ✦ **Computers (open systems servers and/or mainframe) with a host controller, host adapter, or host bus adapter (HBA)**
- ✦ **Storage Arrays with storage network interfaces**
- ✦ **Storage Network Switches**
- ✦ **Cable Plant for Storage Networks**
- ✦ **Storage Management**
- ✦ **Backup Systems (tape, virtual tape, disk)**
- ✦ **Storage Network Gateways**
- ✦ **Network Attached Storage (NAS)**
- ✦ **Fixed Content-aware Storage**
- ✦ **Archive Storage (active archive and long-term archive)**

In-flight versus At-rest



In-flight:

- Two end points (communication)
- Interoperability – network layers
- Data is transitory (temporary)

At-rest:

- Interoperability – media interchangeability
- Data is persistent on media

Very Different Threats and Threat Agents

Storage Ecosystem – Security Challenges

- ✦ **Data Availability Protection (redundancy, resiliency, integrity, performance)**
- ✦ **Data Backup & Recovery (disaster recovery, business continuity)**
- ✦ **Control of Privileged Users (Administrators)**
- ✦ **Protection of Storage Management**
- ✦ **Credential & Trust Management**
- ✦ **Data In-flight Protection**
- ✦ **Data At-rest Protection**
- ✦ **Information Lifecycle Management (ILM)**
- ✦ **Defense & Intelligence (labeled storage, MLS)**
- ✦ **Long-term Archive (access, crypto, authenticity)**

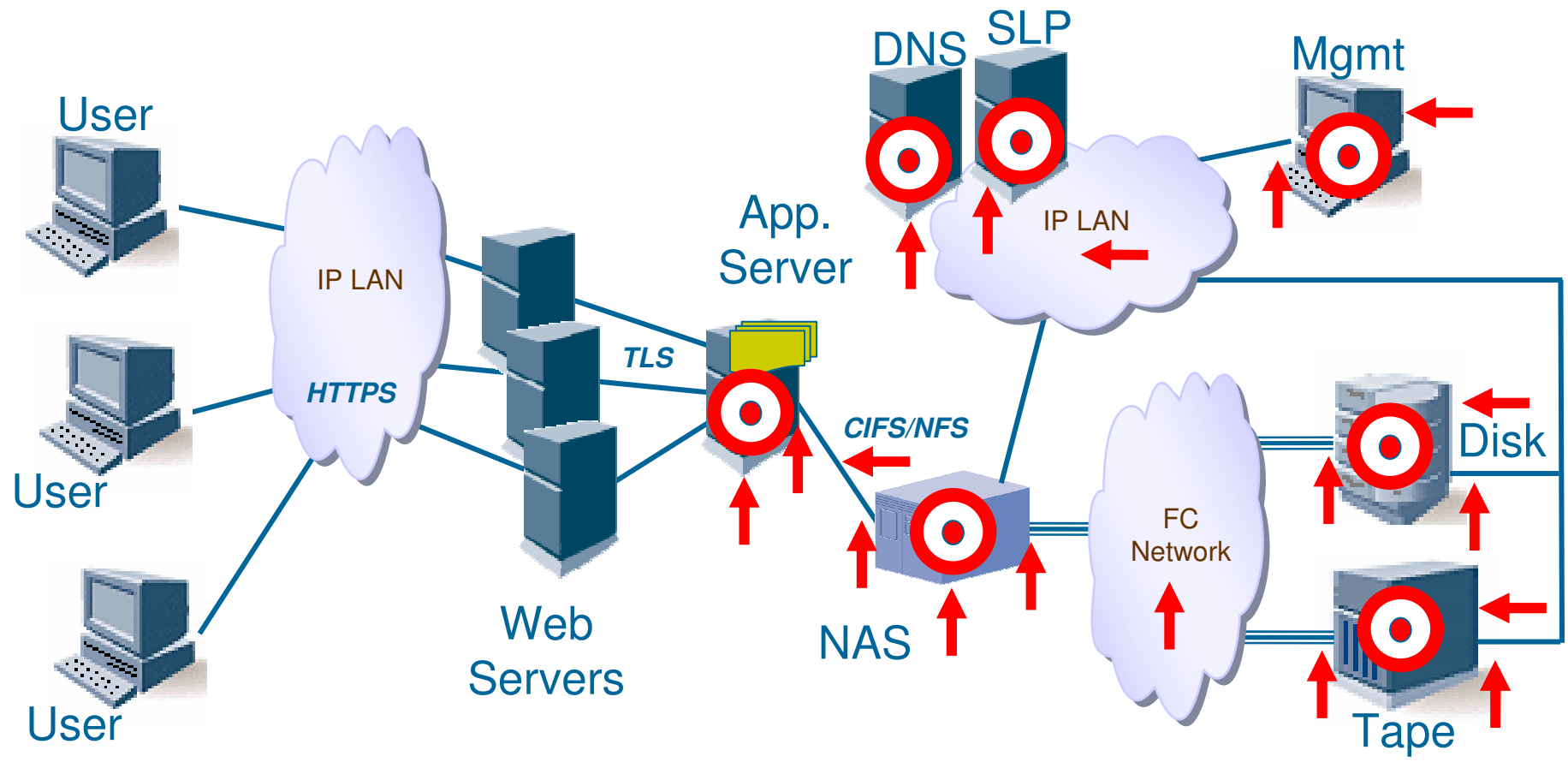




Storage Security Priorities

SNIA Storage Security BCPs

- ✦ **Core (Applicable to Storage Systems/Ecosystems):**
 - ◆ General Storage Security
 - ◆ Storage Systems Security
 - ◆ Storage Management Security
- ✦ **Technology Specific:**
 - ◆ Network Attached Storage (NAS)
 - ◆ Block-based IP Storage
 - ◆ Fibre Channel Storage
 - ◆ Encryption for Storage
 - ◆ Key Management for Storage
 - ◆ Archive Security

Storage Ecosystem Attack Points



 Potential Target  Attack Point

Storage Management

- * **Remember:** Unauthorized and/or uncontrolled management can result in data being destroyed or rendered unavailable
- * **What to Check:**
 - ◆ Compliance with authentication and authorization requirements
 - ◆ Appropriate segregation of management traffic
 - ◆ Use of secure channels for all remote management
 - ◆ Audit logging with full traceability of all privileged user actions
 - ◆ Configuration management practices
 - ◆ Protections against indirect attacks from IT infrastructure
 - ◆ Appropriate controls and monitoring of vendor maintenance
 - ◆ Consistent controls on in-band and out-of-band management
 - ◆ Protections against malware

Network Attached Storage (NAS)

- * **Remember:** Poorly secured NAS (and file servers) can result in unauthorized file sniffing, access, or destruction
- * **What to Check:**
 - ◆ Use of data access protocols with significant security flaws
 - ◆ Network based protections to establish risk domains
 - ◆ Use of secure channels for all remote data access
 - ◆ User-level authentication employed whenever possible
 - ◆ Granting unrestricted (root) access to files on NAS or file server
 - ◆ Enabling multi-protocol (e.g., NFS & CIFS) configurations for users who do not use these services
 - ◆ Protections against malware
 - ◆ Encryption of sensitive files and directories

Internet SCSI (iSCSI)

- ✦ **Remember:** Poorly secured iSCSI storage networks can result in unauthorized data sniffing, access, or destruction
- ✦ **What to Check:**
 - ◆ Network based protections to establish risk domains
 - ◆ Use of entity-based, mutual authentication (CHAP) for all iSCSI initiators and targets
 - ◆ Appropriate segregation of iSCSI traffic for security and performance
 - ◆ Use of IPsec to ensure in-flight confidentiality of sensitive data
 - ◆ Protections against indirect attacks from IT infrastructure

Data Sanitization

- * **Remember:** Poorly executed data sanitization can result in unauthorized disclosure of sensitive data
- * **What to Check:**
 - ◆ Mechanisms actually clear the data residing on the media
 - ◆ Performed in compliance with a data sanitization policy
 - ◆ Sanitization does not violate laws, regulations, or court orders
 - ◆ Sufficient controls to ensure the mechanisms are not attack vectors
 - ◆ Use of “crypto shredding” factors in the strength of the ciphers
 - ◆ Applied to all copies of data residing in backups, at BC/DR sites, in system caches, application caches (e.g., search engines), device mirrors, etc.

Encrypting “Sensitive” Data

✦ Focus on Data Leaving Your Control

- ◆ Data stored on removable media like backup tapes, must be encrypted while at-rest
- ◆ Data stored in third-party (untrusted) data centers must be encrypted both in-flight and at-rest
- ◆ Data transferred between “trusted” data centers must be encrypted in-flight

✦ Encrypting Data At-rest – A measure of last resort

- ◆ Use extreme care when encrypting primary data
- ◆ Long-term key management is a critical element

Encryption of Data At-rest – A Step-by-step Checklist,
http://www.snia.org/forums/ssif/knowledge_center/white_papers/

Final Thoughts

Security and Compliance Balance



Data Security

- * Proactive
- * Defense-in-depth
- * Physical, technical and administrative control areas
- * Preventive, detective and corrective control types

Compliance

- * Reactive
- * Accountability
- * Traceability
- * Monitoring & Reporting
- * Risk Management
- * **Often the driver for security**

Summary

- ✦ **The most significant security risks in storage ecosystems are not perhaps the obvious ones**
- ✦ **Insiders frequently perpetrate the most devastating attacks against data (malicious & accidental)**
- ✦ **Protect critical/sensitive/regulated data when it leaves your control**
- ✦ **Have a plan to deal with data security incidents**
- ✦ **Use a defense-in-depth approach**
- ✦ **Manage the risks **or** mitigate with the consequences**

Last Words

- ✦ Security continues to be a “grudge” expenditure with a focus on “just enough”
- ✦ The storage practitioners and storage industry are just beginning to address security issues, but progress is slow because there are few catalysts for change
- ✦ We the security (and audit) community can be that catalyst



Thank You

eric.hibbard@hds.com