



Education

SNIA Storage Security Best Practices

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

- The material contained in this tutorial is copyrighted by the SNIA.
- 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.

➤ SNIA Storage Security Best Practices

With the increasing importance and emphasis on security in mind, the Storage Networking Industry Association (SNIA) had developed and published (see http://www.snia.org/forums/ssif/programs/best_practices/) a set of storage security best current practices (BCPs). This vendor neutral guidance has a broad scope, covering both storage systems and entire storage ecosystems. Specific elements include, but are not limited to, storage management, protocols, compliance, encryption, key management, and long-term archive. This session provides an introduction to the BCPs as well as information that that will help organizations exploit the BCPs in their own environments.

The 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

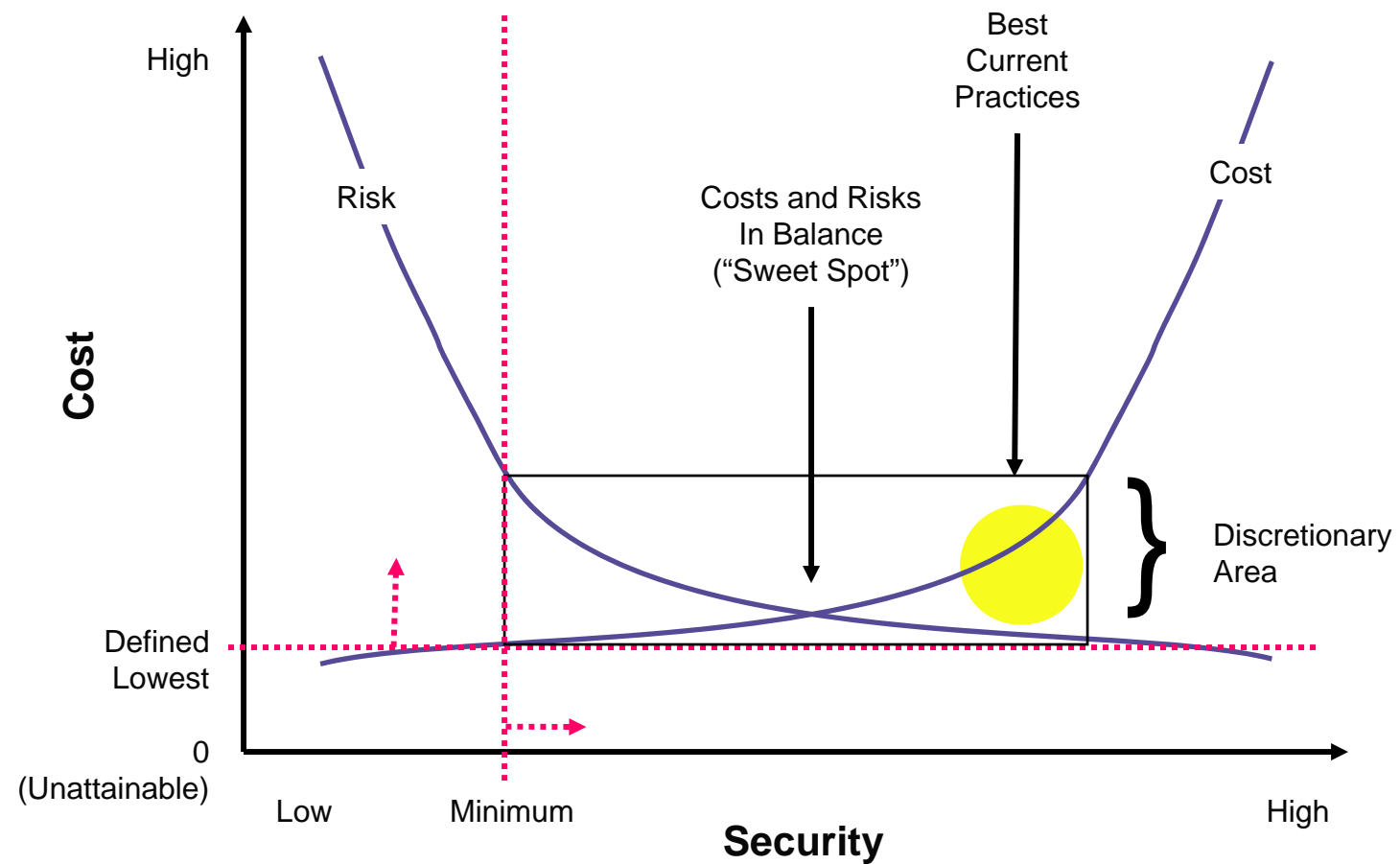
What is Storage Security?

- Technical controls, which may include integrity, confidentiality and availability controls, that protect storage resources and data from unauthorized users and uses. – SNIA Dictionary
- It represents the **convergence** of the storage, networking, and security disciplines, technologies, and methodologies for the purpose of protecting and securing digital assets.
- Storage security is simply a part of information assurance, which includes measures that protect and defend information and information systems by ensuring their confidentiality, integrity, availability, access control and nonrepudiation. Information assurance encompasses system reliability and strategic risk management, and includes providing for restoration of information systems using protection, detection, and reaction capabilities.

What are Best Practices?

- Best practice is an idea that asserts that there is a technique, method, process, activity, incentive or reward that is more effective at delivering a particular outcome than any other technique, method, process, etc. The idea is that with proper processes, checks, and testing, a desired outcome can be delivered with fewer problems and unforeseen complications. Best practices can also be defined as the most efficient (least amount of effort) and effective (best results) way of accomplishing a task, based on repeatable procedures that have proven themselves over time for large numbers of people. - Wikipedia
- For the purpose of the SNIA storage security best practices, they provide broad guidance to organizations seeking to secure their individual storage systems as well as their storage ecosystems.

Balancing Cost & Security



© 1996 – 2000 Ray Kaplan All Rights Reserved

Source: Ray Kaplan, CISSP, *A Matter of Trust*, Information Security Management Handbook, 5th Edition. Tipton & Krause, editors.

SNIA Storage Security Best Current Practices (BCPs)

SOURCE: Storage Networking Industry Association Technical Proposal, *SNIA Storage Security – Best Current Practices (BCPs) Version 2.1.0*, © 2008 by SNIA, http://www.snia.org/forums/ssif/programs/best_practices/

Background

- Developed by the SNIA Security TWG
- Documented in a SNIA Technical Proposal
- Guidance is provided in a vendor neutral manner
- Written in layman terms, avoiding unnecessary storage- or security-specific jargon and acronyms
- Assume a basic working knowledge of practices and concepts of either storage or security
- Target audience includes practitioners, IT architects, IT managers, and corporate executives

Introduction to the BCPs

- They cover both storage systems and entire storage ecosystems
- Grouped into categories:
 - ◆ **core** – apply to all storage systems/ecosystems and they cover basic storage security elements
 - ◆ **technology specific** – above and beyond the core BCPs and they may or may not apply. When they do apply, multiple categories of the technology specific BCPs may be applicable for a given environment

Using the BCPs

- They are not a checklist; they do not represent a minimum set of requirements to determine compliance
- A balance must be struck between mitigating risks and minimizing the impacts, which may take the form of cost, complexity, throughput, availability, scalability, etc.
- Each organization must make its own trade-off decisions based on its unique situation (e.g., deployed infrastructure, legal and regulatory requirements, and due care expectations) and the importance of its data

Structure of 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
- ◆ Long-term Information Security

Core - General Storage Security

- GEN01 – Identify & Assess All Storage Interfaces
- GEN02 – Create Risk Domains
- GEN03 – Monitor & Control Physical Access
- GEN04 – Avoid Failures Due to Common Mistakes
- GEN05 – Address Data Security Compliance
- GEN06 – Implement Appropriate Service Continuity
- GEN07 – Align Storage and Policy

Commentary: Core - General

- Have a clear understanding of the assets involved (technology and data) as well as a basic classification.
- Use risk domains to limit access and damage
- Ensure that virtualization doesn't create undesired risks to data
- Physical access can be hazardous to data
- Never underestimate the damage from incompetence or foolishness
- Compliance is a major driver for security, so pay attention to accountability, traceability, risk management, retention & sanitization, privacy, and legal requirements.
- Make sure storage participates in the survivability measures
- Ensure storage participates in and complies with policy

Core - Storage Systems Security BCPs

- SSS01 – Understand the exposures
- SSS02 – Utilize Event Logging
- SSS03 – Secure Backups and Replication
- SSS04 – Use Trusted and Reliable Infrastructure

Commentary: Core - Systems

- Understand the security posture of your storage systems/ecosystems and adjust appropriately
- Ensure storage participates in the centralized audit logging and meets the evidentiary requirements (if any)
- Ensure that backups and replication don't become a source of unauthorized data access or disclosure
- Avoid attacks and failures because of infrastructure dependencies

Storage Management Security BCPs

- SMS01 – Secure the Management Interfaces
- SMS02 – Harden Management Applications
- SMS03 – Tightly Control Access and Privileges
- SMS04 – Restrict Remote Support
- SMS05 – Include Configuration Management

Commentary: Core - Management

- Protect the management interfaces from unauthorized access and reconnaissance to avoid data destruction, corruption, and denial of access.
- Thou shalt control and monitor your vendor access to storage systems
- Implement least privilege controls and separation of duties for privileged users
- Ensure that remote support is performed securely and in compliance with policy
- Employ change controls and configuration management practices

➤ NAS01 – Network File System (NFS)

- ◆ NAS01.A Control NFS Network Access and Protocols
- ◆ NAS01.B Apply Access Controls to NFS Exported Filesystems
- ◆ NAS01.C Restrict NFS Client Behaviors
- ◆ NAS01.D Secure Data on NFS Filer

➤ NAS02 – SMB/CIFS

- ◆ NAS02.A Control SMB/CIFS Network Access and Protocols
- ◆ NAS02.B Apply Access Controls to SMB/CIFS Exported Filesystems
- ◆ NAS02.C Restrict SMB/CIFS Client Behaviors
- ◆ NAS02.D Secure Data on SMB/CIFS Filer

Commentary: Tech - NAS

- If your file access protocols (NFS, SMB, CIFS, HTTP, NCP) are poorly secured, the data can be accessed, sniffed, or destroyed at-will
- Employ user-level authentication whenever possible (e.g., NFSv4 with Kerberos V5)
- Avoid granting “root” or “administrator” unrestricted access to files on NAS or file server
- Only enable multi-protocol (e.g., NFS & CIFS) access for those users who use these services

Tech – Block-based IP Storage BCPs

➤ IPS01 – Secure iSCSI

- ◆ IPS01.A Control iSCSI Network Access and Protocols
- ◆ IPS02.B Implement iSCSI Security Measures

➤ IPS02 – Secure FCIP

- ◆ IPS01.A Control FCIP Network Access and Protocols
- ◆ IPS02.B Implement FCIP Security Measures

Commentary: Tech - IP

- CHAP authentication is available in all iSCSI implementations (initiators and targets), so use it
- Avoid connecting iSCSI and FCIP interfaces to general purpose LANs; segregate for security and performance
- VLANs are not the same as physically isolated LANs
- Use IPsec to secure the communication channel when sensitive data could be exposed

Tech – Fibre Channel Storage BCPs

- **FCS01 Secure FCP**
 - ◆ FCS01.A Control FCP Node Access
 - ◆ FCS01.B Implement FCP Security Measures
- **FCS02 Secure Fibre Channel Storage Networks**
 - ◆ FCS02.A Implement Switch-based Controls
 - ◆ FCS02.B Interconnect Storage Networks Securely

Commentary: Tech - FC

- Limit access to storage, using WWN-based access controls (LUN masking and zoning)
- Leverage ANSI 426–2007 FC-SP features (like authentication and in-flight encryption) for trusted in-band management and trusted storage networks
- Restrict switch interconnections (e.g., ACLs, binding lists, FC-SP policy)
- Configure switches, extenders, routers, and gateways (e.g., FCIP and FC-to-iSCSI) with the least amount of access

Tech – Encryption for Storage BCPs

- ❖ **ENC01 – Protect Externalized Data**
 - ◆ ENC01.A Secure Sensitive Data on Removable Media
 - ◆ ENC01.B Secure Sensitive Data Transferred Between Data Centers
 - ◆ ENC01.C Secure Sensitive Data in 3rd-party Data Centers
- ❖ **ENC02 – Pedigree of Encryption**
 - ◆ ENC02.A Encryption Algorithms
 - ◆ ENC02.B Symmetric Encryption Modes
 - ◆ ENC02.C Strength of Encryption
- ❖ **ENC03 – Risk Assessment in Use of Encryption**
 - ◆ ENC03.A Identify and Classify Sensitive Data
 - ◆ ENC03.B Analyze Risks and Protection Options
 - ◆ ENC03.C Mitigate Risks with Encryption
- ❖ **ENC04 – Encryption Issues**
 - ◆ ENC04.A Point of Encryption
 - ◆ ENC04.B Align with Data Reduction Services
 - ◆ ENC04.C Proof of Encryption

Commentary: Tech - Encryption

- SNIA position on encryption:
 - ◆ Off-site backup tapes of sensitive/regulated data must be encrypted; encryption keys stored separately
 - ◆ Data transferred to remote datacenters must be encrypted in-flight when sensitive/regulated
 - ◆ Sensitive/regulated data stored in third-party datacenters must be encrypted prior to arrival
- Treat at-rest encryption of primary data as a measure of last resort
- Ensure the pedigree of the encryption is up to the job
- Ensure that encryption is driven by appropriate risk analysis and business need
- Avoid huge challenges by identifying the appropriate point of encryption, aligning the encryption with data reduction mechanisms, and creating appropriate audit trails

Tech – Key Management BCPs

- **KMS01 – Key Management Principles**
 - ◆ KMS01.A Observe Important Properties of Keys
 - ◆ KMS01.B Implement and Use Key Management Safely
- **KMS02 – Key Management Functions**
 - ◆ KMS02.A Establish Keys Securely
 - ◆ KMS02.B Ensure Proper Operational Use
 - ◆ KMS02.C Key Disposition
- **KMS03 – Key Management Issues**
 - ◆ KMS03.A Comply with Import/Export Controls
 - ◆ KMS03.B Plan for Problems

Commentary: Tech – Key Management

- Key management is the more difficult aspect of cryptograph and standards continue to lag
- Adhere to basic principles associated with keying material as well as implementing key management
- Understand and obey government **import** and **export** regulations associated with encryption and key management
- Consider escrowing keying material used to protect business/mission critical information

Tech – Long-term Security BCPs

- **ARC01 – On-line Fixed Content**
 - ◆ ARC01.A Secure the On-line Fixed Content
 - ◆ ARC01.B Provide Governance and Compliance Functionality

- **ARC02 – Off-line Fixed Content**
 - ◆ ARC02.A Establish Off-line Fixed Content Policy
 - ◆ ARC02.B Maintain Off-line Fixed Content Security

Commentary

- Establish and enforce data retention requirements, including Legal Hold requirements (e.g., e-Discovery)
- Preserve the evidentiary nature of the data through the careful use of authenticity, integrity, and chain of custody mechanisms
- Identify the types of data to be accepted as well as the preservation period (e.g., not longer than 30 years)
- Ensure that the cryptographic assurances of confidentiality and authenticity are maintained

Final Thoughts

- 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 is basically a people problem... computers don't just wake up and start attacking their neighbors on their own...at least not yet!
- It is not a matter of **IF** you will be attacked, but rather **WHEN** and if you will **KNOW** that you have been attacked.

- Please send any questions or comments on this presentation to SNIA: tracksecurity@snia.org

**Many thanks to the following individuals
for their contributions to this tutorial.**

- SNIA Education Committee

**Eric A. Hibbard, CISSP, CISA
Larry Hofer, CISSP
Roger Cummings
LeRoy Budnik, CISA
SNIA Security TWG**

**Richard Austin, CISSP
Andrew Nielsen, CISSP, CISA
Phil Huml
Ray Kaplan, CISSP**

For More Information

- **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/security/
- **Storage Security Industry Forum (SSIF)**
 - ◆ **Focus:** Marketing collateral, educational materials, customer needs, whitepapers, and best practices for storage security.
 - ◆ <http://www.snia.org/ssif>