



Education

# Introduction to Storage Security

Andrew Nielsen, CISSP, ISSAP, INAL  
Hitachi Data Systems

# SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA.
- Member companies and individuals may use this material in presentations and literature under the following conditions:
  - ◆ Any slide or slides used must be reproduced without modification
  - ◆ The SNIA must be acknowledged as 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.

## Introduction to Storage Security

Many enterprises face the task of implementing data protection and data security measures to meet a wide range of requirements. We have already made you aware of the threats. You know that the risks and threats are real; it is just a matter of time before you become a statistic. The security best practices provided by the SNIA Security Technical Work Group will help you to secure the storage infrastructure to know and manage our risks. However, what will it really take to implement a secure storage infrastructure? What upfront work is required to implement security? What is the ongoing work to insure that the storage infrastructure is secure?.

# Session Overview

- This session focuses on the efforts required at the storage layer to create a successful defense-in-depth strategy. Major threats for each of the key storage element are explored. The session provides information on how to determine the security posture of these elements in a particular installation. However, be aware that the session leverages material contained in the SNIA-SSIF whitepaper: Introduction to Storage Security. This enables the session to expand further on these concepts.
  
- **Learning Objectives:**
  - ◆ Know storage security measures in response to risk and threat
  - ◆ Apply best practices for data protection and security
  - ◆ Understand the upfront and continuing effort required to secure the storage layer

- Concepts Overview
  - ◆ Security
  - ◆ Compliance
- Where to Start
- Best Practices
- Final Words
  
- Additional Information

# Concepts Overview

**SOURCE:** SNIA/Storage Security Industry Forum (SSIF), *Introduction to Storage Security*,  
© 2005 by SNIA, <http://www.snia.org/ssif/documents>

# Drivers for Data-centric Security

- Data Created at Exponential Growth Rates
- On-going Attacks from Internal/External Sources
- Data Protection/Privacy Regulations
- Data Retention and Destruction Regulations
- Increased Access to Data
- Increased Use of Automation
- Transfer of Services Down the Stack into the Storage Layers
- Concentration of information in high density storage devices creates a few, highly valuable targets

# Primary Security Services

- **Access Control** – Preventing the unauthorized use of networked resources and data as well as the unauthorized disclosure or modification of data. It includes identification, authentication and authorization.
- **Confidentiality** – Preventing unauthorized disclosure of data (both stored and communicated). It includes data protection, data separation, and traffic flow protection (frequency, quantity, destination of traffic flow, etc.).
- **Integrity** – Guarding against improper modification or destruction of information as well as assuring non-repudiation and authenticity. It includes prevention of unauthorized modification of data (both stored and communicated), detection and notification of unauthorized modification of data, and recording of all changes to data.
- **Availability** – Ensuring timely and reliable access to and use of data and information services for authorized users. A loss of availability is the disruption of access or use of information or an information system. It includes protection from attacks, unauthorized use, and resilience to routine failures.
- **Nonrepudiation** – Repudiation is denial by one of the entities involved in a communication that it participated in that communication. The nonrepudiation security service provides the ability to prove to a third party that the entity did indeed participate in the communication.

## ➤ Security Requires

- ◆ Auditability and Accountability
- ◆ Access Control
- ◆ Confidentiality
- ◆ Integrity
- ◆ Asset Availability

## ➤ Security is an Integral Element of Sound Management

## ➤ Security Should be Cost-effective

## ➤ Security also requires

- ◆ Risk Management
- ◆ Comprehensive and Integrated Approach
- ◆ Life-cycle Management

## ➤ Security Responsibilities and Accountability Should Be Made Explicit



# Basic Security Concepts & Principles (cont.)

## ➤ Security Requires

- ◆ Training and Awareness
- ◆ Continual Reassessment

## ➤ Security Must Respect Ethical and Democratic Rights

## ➤ Other Basic Security Principles

- ◆ Choke point
- ◆ Consistency
- ◆ Control of the periphery
- ◆ Defense in depth

- ◆ Deny upon failure
- ◆ Diversity of defense
- ◆ Interdependency
- ◆ Override
- ◆ Reliability
- ◆ Simplicity
- ◆ Timeliness
- ◆ Universal applicability/participation
- ◆ Weakest link

# What is Compliance?

- The state of being in accordance with legal, regulatory, financial, and/or business “authorities” and their requirements.
- Requirements are often vague and subject to interpretation (e.g., current best practices)
- An organization’s alignment and/or fulfillment of these requirements is usually determined by external third parties (i.e., auditors)
- Non-compliance can have significant, negative consequences

# Regulatory Drivers (Domestic US)

- Sarbanes-Oxley (SOX) Act
- Gramm-Leach-Bliley Act (GLBA)
- Securities Exchange Act (SEC) Rules 17a-3 and 17a-4
- California Data Security Act (SB 1386/AB 1950)
- Health Insurance Portability & Accountability Act (HIPAA)
- DOE 10 CFR 600.153 Retention & Access Requirements for Records
- U.S. Patriot Act
- International Trafficking in Arms Regulations (ITAR)
- Food & Drug Administration (FDA): Title 21 CFR Part 11
- Homeland Security Information Sharing Act (HSISA)
- New York Reg. 173

- European Union Data Protection Directive of 1995
- Basel Capital Accord (Basel II)
- EU Directive on Telecommunication Privacy
- Canada: Personal Information Protection and Electronic Documents Act (PIPEDA)
- Australia: Commonwealth Privacy Act 1988
- Japanese Protection for Personal Information Act
- UK: Data Protection Act 1998
- New Zealand: Privacy Act 1993

# Auditor Angle – Standard of Care

- Due Diligence – responsibility one has to investigate and identify issues
  - ◆ Are the risks managed appropriately
  - ◆ Are the “sensitive” information assets protected appropriately
  - ◆ Are the “critical” information assets protected appropriately
- Due Care – doing something about the findings from due diligence
  - ◆ Risk treatment passes the “giggle” test
  - ◆ Information protection and information security measures are reasonable (i.e., in line with those of peers)
  - ◆ Can we prove that security measures were active at the time of an incident
- ROI = Risk of Incarceration

# Where to Start



## Data Security

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

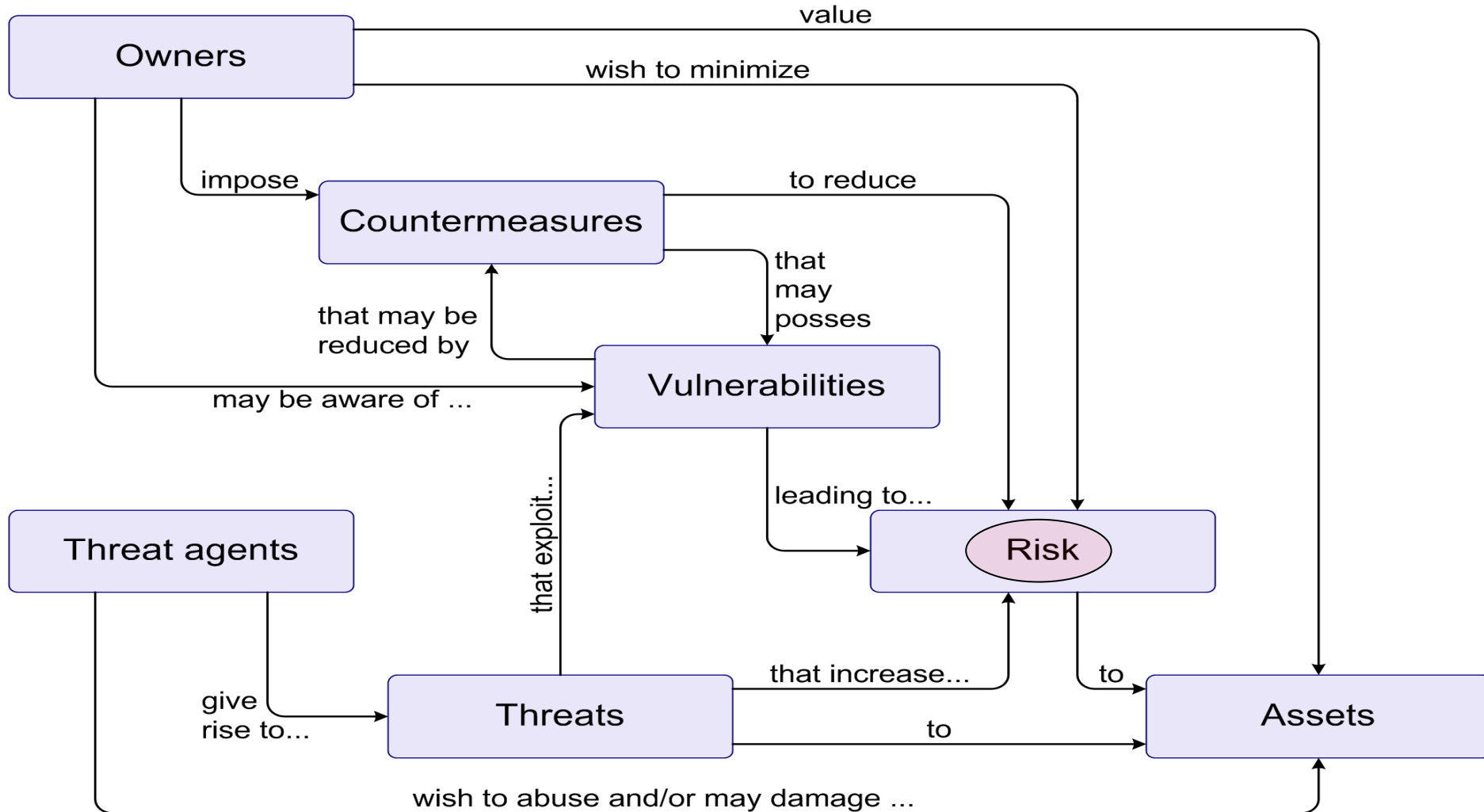
## Compliance

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

# Leverage Security Frameworks

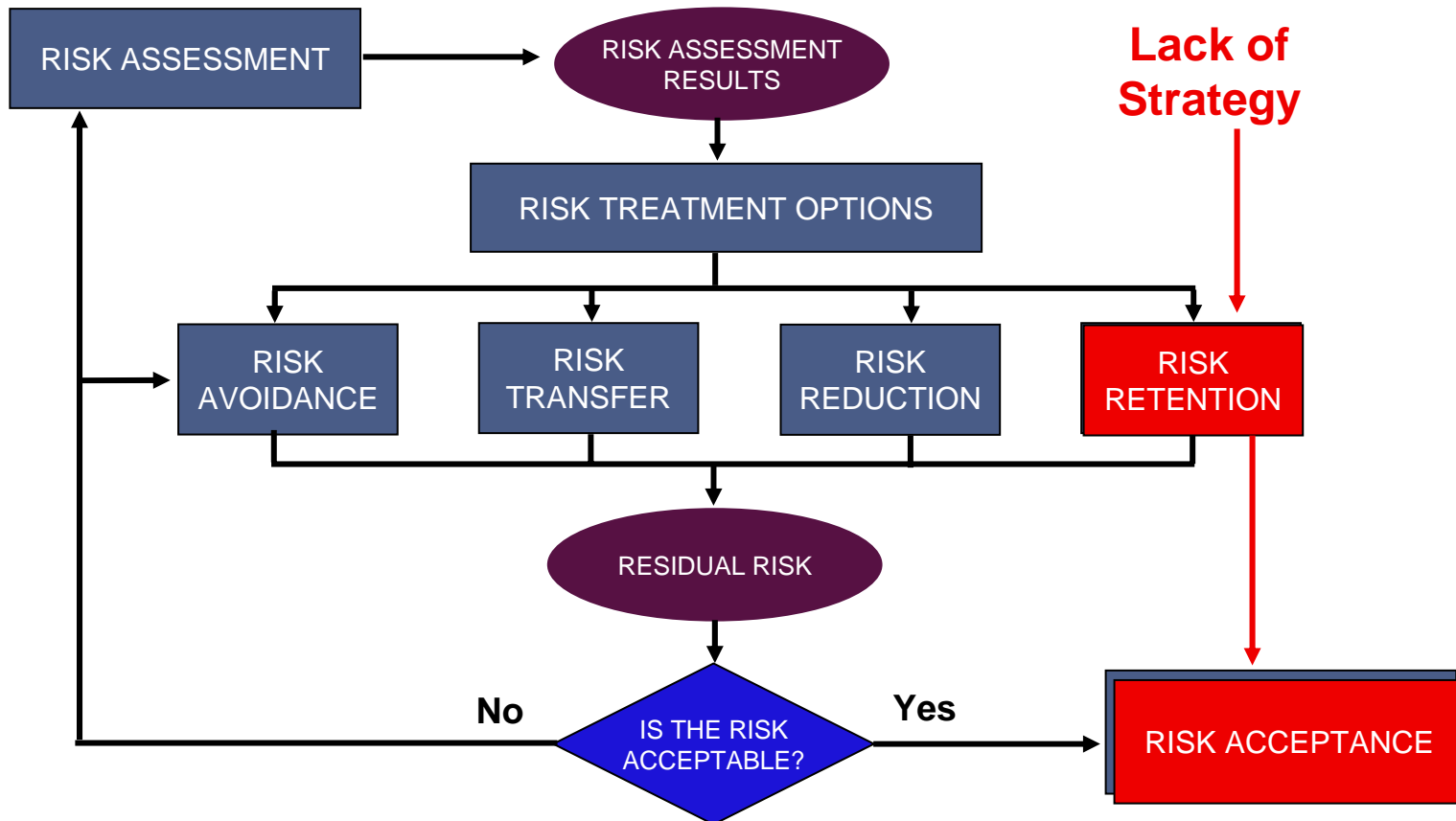
- ISO/IEC 27001:2006 Information Security Management - Requirements & ISO/IEC 27002:2005 (17799:2005) The Code of Practice for Information Security Management
- IT Governance Institute (ITGI), Control Objectives for Information and related Technology (COBIT) Version 4.0
- Committee of Sponsoring Organizations (COSO) of the Treadway Commission
- Federal Financial Institutions Examination Council (FFIEC)
- National Institute of Standards and Technology (NIST), Recommended Security Controls for Federal Information Systems (Special Publication 800-53)
- Canadian Institute of Chartered Accountants (CICA), Information Technology Control Guidelines (ITCG)
- UK Office of Government Commerce (OGC), Information Technology Infrastructure Library (ITIL), Security Management

# The Security “Big Picture”



- Disclosure or unauthorized access
- Deception or acceptance of falsified data
- Disruption or interruption or prevention
- Usurpation or unauthorized control
- Snooping (unauthorized interception)
- Modification or alteration
  - ◆ Active wiretapping
  - ◆ Man-in-the-middle attacks
- Masquerading or spoofing
- Repudiation of origin
- Denial of receipt
- Delay
- Denial of Service
- Environmental (floods, earthquakes, backhoes, etc.)

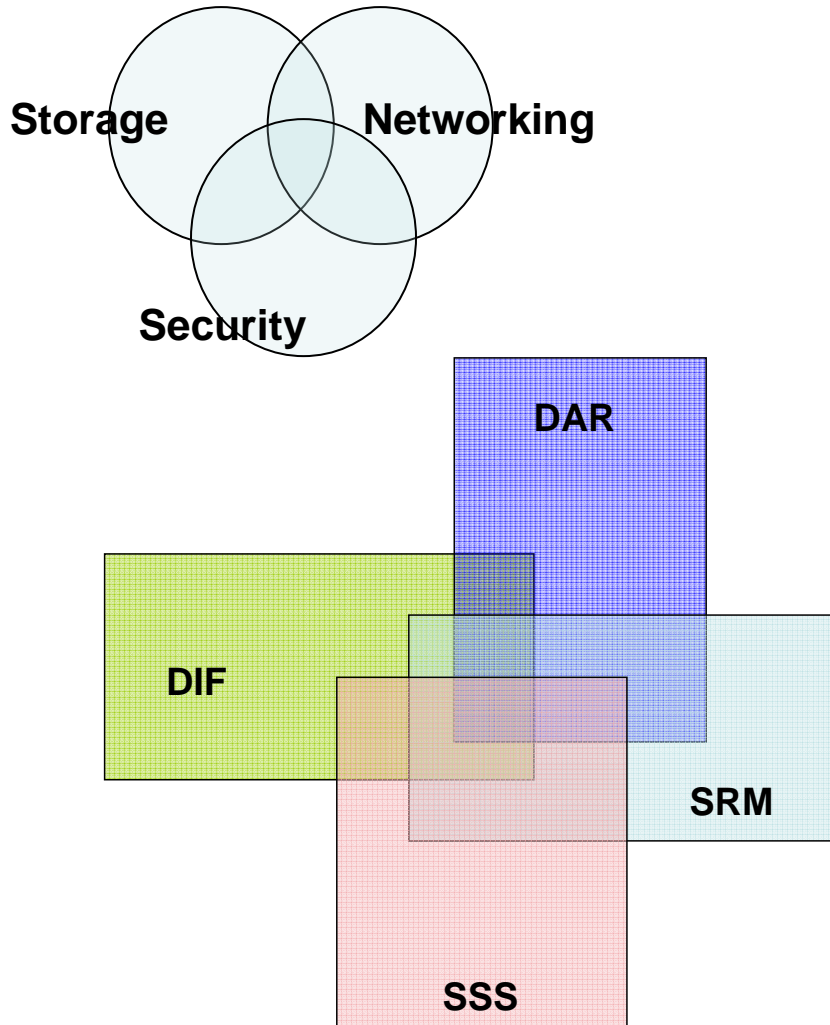
# Strategic Risk Management



# SNIA Storage Security Best Current Practices (BCPs)

**SOURCE:** SNIA/Storage Security Industry Forum (SSIF), *SNIA Storage Security – Best Current Practices (BCPs) Version 2.0*, © 2007 by SNIA,  
<http://www.snia.org/ssif/documents>

# Elements of Storage Security



**Storage System Security (SSS)** – Securing underlying/embedded systems and applications as well as integration with IT and security infrastructure (e.g., external authentication services, centralized logging, firewalls, etc.).

**Storage Resource Management (SRM)** – Securely provisioning, monitoring, tuning, re-allocating, and controlling the storage resources so that data may be stored and retrieved (i.e., all storage management).

**Data In-Flight (DIF)** – Protecting the confidentiality, integrity and/or availability of data as they are transferred across the storage network, the LAN, and the WAN.

**Data At-Rest (DAR)** – Protecting the confidentiality, integrity and/or availability of data residing on servers, storage arrays, NAS appliances, tape libraries, and other media (especially removable).

# 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
  - ◆ Archive Security

# General Storage Security BCPs

- GEN01 – Identify & Assess All Storage Interfaces
  - ◆ GEN01.A Identify physical & logical interfaces
  - ◆ GEN01.B Inventory physical & logical interfaces
  - ◆ GEN01.C Classify Sensitive & Critical Interfaces
- GEN02 – Create Risk Domains
  - ◆ GEN02.A Physical
  - ◆ GEN02.B Logical
- GEN03 – Monitor & Control Physical Access
  - ◆ GEN03.A Facilities
  - ◆ GEN03.B Network Infrastructure & Cable plant
  - ◆ GEN03.C Storage resources

- GEN04 – Avoid Failures Due to Common Mistakes
  - ◆ GEN04.A Software configurations
  - ◆ GEN04.B Maintenance
  - ◆ GEN04.C Access Controls
- GEN05 – Address Data Security Compliance
  - ◆ GEN05.A Accountability
  - ◆ GEN05.B Traceability
  - ◆ GEN05.C Risk Management
  - ◆ GEN05.D Detect, Monitor, and Evaluate
  - ◆ GEN05.E Information Retention & Sanitization
  - ◆ GEN05.F Privacy

- GEN06 – Implement Appropriate Service Continuity
  - ◆ GEN06.A Disaster Recovery (DR)
  - ◆ GEN06.B Business Continuity (BC)
  - ◆ GEN06.C Planning & Testing
- GEN07 – Align Storage and Policy
  - ◆ GEN07.A Incorporate Storage in Policies
  - ◆ GEN07.B Conformance with Policies

# Storage Systems Security BCPs

- **SSS01 – Understand the exposures**
  - ◆ SSS01.A Perform Vulnerability Assessments
  - ◆ SSS01.B Maintain Security of Systems
  - ◆ SSS01.C Monitor for Zero-day Events
- **SSS02 – Utilize Event Logging**
  - ◆ SSS02.A Include Storage in Logging Policy
  - ◆ SSS02.B Employ External Event Logging
  - ◆ SSS02.C Ensure Complete Event Logging
  - ◆ SSS02.D Implement Appropriate Retention and Protection

- SSS03 – Secure Backups and Replication
  - ◆ SSS03.A Backup Security
  - ◆ SSS03.B Replication Security
- SSS04 – Use Trusted and Reliable Infrastructure
  - ◆ SSS04.A Use Trusted Services
  - ◆ SSS04.B Minimize Impacts of Failures
  - ◆ SSS04.C Limit Dynamic Discovery

- **SMS01 – Secure the Management Interfaces**
  - ◆ SMS01.A Segregate Out-of-band Management
  - ◆ SMS01.B Restrict In-band Management
  - ◆ SMS01.C Control Vendor Maintenance
- **SMS02 – Harden Management Applications**
  - ◆ SMS02.A Administrative Consoles and Management Applications
  - ◆ SMS02.B SMI-S Access
  - ◆ SMS02.C SNMP Access
  - ◆ SMS02.D Command Line Interface (CLI) Access
  - ◆ SMS02.E Web-based Access

- **SMS03 – Tightly Control Access and Privileges**
  - ◆ SMS03.A Configure Administrative Accounts
  - ◆ SMS03.B Use Good Access Control Practices
- **SMS04 – Restrict Remote Support**
  - ◆ SMS04.A Limit access to dial in modems
  - ◆ SMS04.B Control Remote Network Access
- **SMS05 – Include Configuration Management**
  - ◆ SMS05.A Baseline Configurations
  - ◆ SMS05.B Institute Operational CM

# Network Attached Storage BCPs

## ➤ 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

# 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

# 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

# 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 3<sup>rd</sup>-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

- **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

## ➤ ARC01 – Active Archive

- ◆ ARC01.A Secure the Active Archive
- ◆ ARC01.B Provide Governance and Compliance Functionality

## ➤ ARC02 – Long-term Archive

- ◆ ARC02.A Establish Long-term Archive Policy
- ◆ ARC02.B Maintain LTA Security

# Final Thoughts

- The most significant security risks in storage networks are not perhaps the obvious ones
  - ◆ Attacks via out-of-band interfaces
  - ◆ Threats in the data center
- 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

- 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](mailto:tracksecurity@snia.org)

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

*SNIA Education Committee*

**Eric A. Hibbard, CISSP  
Andrew Nielsen, CISSP  
LeRoy Budnik, CISA  
Phil Huml**

**Larry Hofer CISSP  
Richard Austin, CISSP  
Roger Cummings**

**SNIA Security TWG**

**SNIA SSIF**

# 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/](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>



# Relevant Storage Security Standards Bodies

- ISO/IEC JTC1 SC27 ([www.din.de/ni/sc27](http://www.din.de/ni/sc27)) – IT Security Techniques
- NIST/CSD Computer Security Resource Center ([csrc.nist.gov](http://csrc.nist.gov)) – Security standards for US Government
- IEEE/P1619 ([siswg.net](http://siswg.net)) – Security in Storage Working Group
- INCITS T10 ([www.t10.org](http://www.t10.org)) – SCSI security, tape drive encryption control etc.
- INCITS T11 ([www.t11.org](http://www.t11.org)) – Fibre Channel security
- IETF ([www.ietf.org](http://www.ietf.org)) – IP security (IPsec), Transport Layer Security (TLS)

# Security Framework Sources

- ISO/IEC 27001/27002 ([www.iso.org](http://www.iso.org)) – Information security management systems
- COBIT® ([www.isaca.org/cobit](http://www.isaca.org/cobit)) – Control Objectives for Information and related Technology
- COSO ([www.coso.org](http://www.coso.org)) – Enterprise Risk Management — Integrated Framework
- FFIEC ([www.ffiec.gov](http://www.ffiec.gov)) – FFIEC Information Technology Examination Handbook
- NIST/CSD Computer Security Resource Center ([csrc.nist.gov/publications/nistpubs](http://csrc.nist.gov/publications/nistpubs)) – Security standards for U.S. Government
- CICA ([www.cica.ca](http://www.cica.ca)) – Information Technology Control Guidelines (ITCG)
- ITIL ([www.itil.co.uk](http://www.itil.co.uk)) – ITIL Security Management

# Web Sources of Information

- The CERT® Coordination Center, <http://www.cert.org>
- The SANS (SysAdmin, Audit, Network, Security) Institute, <http://www.sans.org>
- The Center for Internet Security (CIS), <http://www.cisecurity.org>
- Information Systems Audit and Control Association (ISACA) – *IS Standards, Guidelines, and Procedures for Auditing and Control Professionals*, <http://www.isaca.org/standards/>
- Information Security Forum (ISF) – The Standard of Good Practice for Information Security, <http://www.isfsecuritystandard.com/>
- Open Information Systems Security Group (OISSG), <http://www.oissg.org>
- Open Web Application Security Project (OWASP), <http://www.owasp.org>