



Education

# **Preparing for a Security Audit: Best Practices for Storage Professionals**

Blair Semple, CISSP-ISSEP  
Vice Chair, SNIA Storage Security Industry Forum,  
Security Evangelist, NetApp

- 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.**

# Preparing for a security audit

- Until recently being in compliance with security requirements and having materials available for a security audit may not have been part of your job as a storage administrator, but times have changed. As a storage administrator what best practices can you employ to :
  1. know what may be required from you during a security audit
  2. what data collection should you be doing to be prepared for an audit
  3. what procedures and processes should you be implementing to make the audit go smoothly
  4. what are the capabilities and solutions you should look for to help in producing the materials required by an audit
  
- This tutorial focuses on practical advice for storage administrators and does not assume a security background. At the end of the session you should have a set of guidelines for meeting your requirements around preparing for, going through, and avoiding the pitfalls that could result from the audit.

- This presentation presents a view of the storage security best practices as developed by the SNIA
- A source for the storage security best practices is:
- [http://www.snia.org/forums/ssif/programs/best\\_practices](http://www.snia.org/forums/ssif/programs/best_practices)

# What's Required to Survive an Audit?

# Your Primary Strategy

- Its good to be a Boy Scout
  - ◆ Be Prepared - With some forethought and the right data you will survive
  
- Understand the focus areas and requirements
  
- Storage is likely to be a consideration, but not the exclusive domain of the audit. So,
  
- Interface with your peers in other facets of the audit.

- Understand the nature of requirements you must meet
  - ◆ May depend upon:
    - > Your specific industry
    - > The nature of your organization
    - > Your location
  
- Documentation of you processes and procedures in meeting those controls
  - ◆ Are they automated or manual
  - ◆ What are type of reporting cycles are required?

# Areas of Consideration

- What type of evidence will you need
  - ◆ Physical
  - ◆ Electronic
  - ◆ Real-time monitoring
  - ◆ Its always important to collect and maintain records and audit logs – auditors can often help identify
- Understand remaining areas of improvement
  - ◆ Be able to demonstrate any compensating controls to cover any gaps
- Determine adherence to policy

# Some Industry-Specific Regulations

## ➤ Health care, Insurance

- ◆ Health Insurance Portability and Accountability (HIPAA)
- ◆ 6 year retention of audit information

## ➤ Finance

- ◆ Basel II accord – risk management practices
- ◆ 3-7 year audit retention

## ➤ Publically-traded companies

- ◆ Sarbanes Oxley (SOX) Act
- ◆ Audit of unauthorized access, misuse, fraud in order to ensure the accuracy of corporate financial and business information
- ◆ 7 year retention period

## ➤ Retail, financial services

- ◆ Payment Card Industry – Data Security Standards (PCI-DSS)

## ➤ Anywhere customer data is collected and stored

- ◆ Privacy disclosure laws, EU privacy directive

# Privacy disclosure laws

## ➤ If you lose control of physical media

- ◆ Do your governing regulations provide a “Safe Harbor” when data is encrypted?
  - Can you supply irrefutable logs indicating data was secured:
    - What encryption method was used,
    - Time and location the encryption occurred,
    - What key identifier was used?
- ◆ Was the data cleansed by overwrite?
  - When? Where? Using what method?
- ◆ Was it degaussed or shredded?
  - Document, Document, Document

# Making your position defensible

## ➤ Could you prove:

- ◆ What data or object was affected?
- ◆ What action was performed?
- ◆ When was it executed?
- ◆ Who authorized and performed the action?

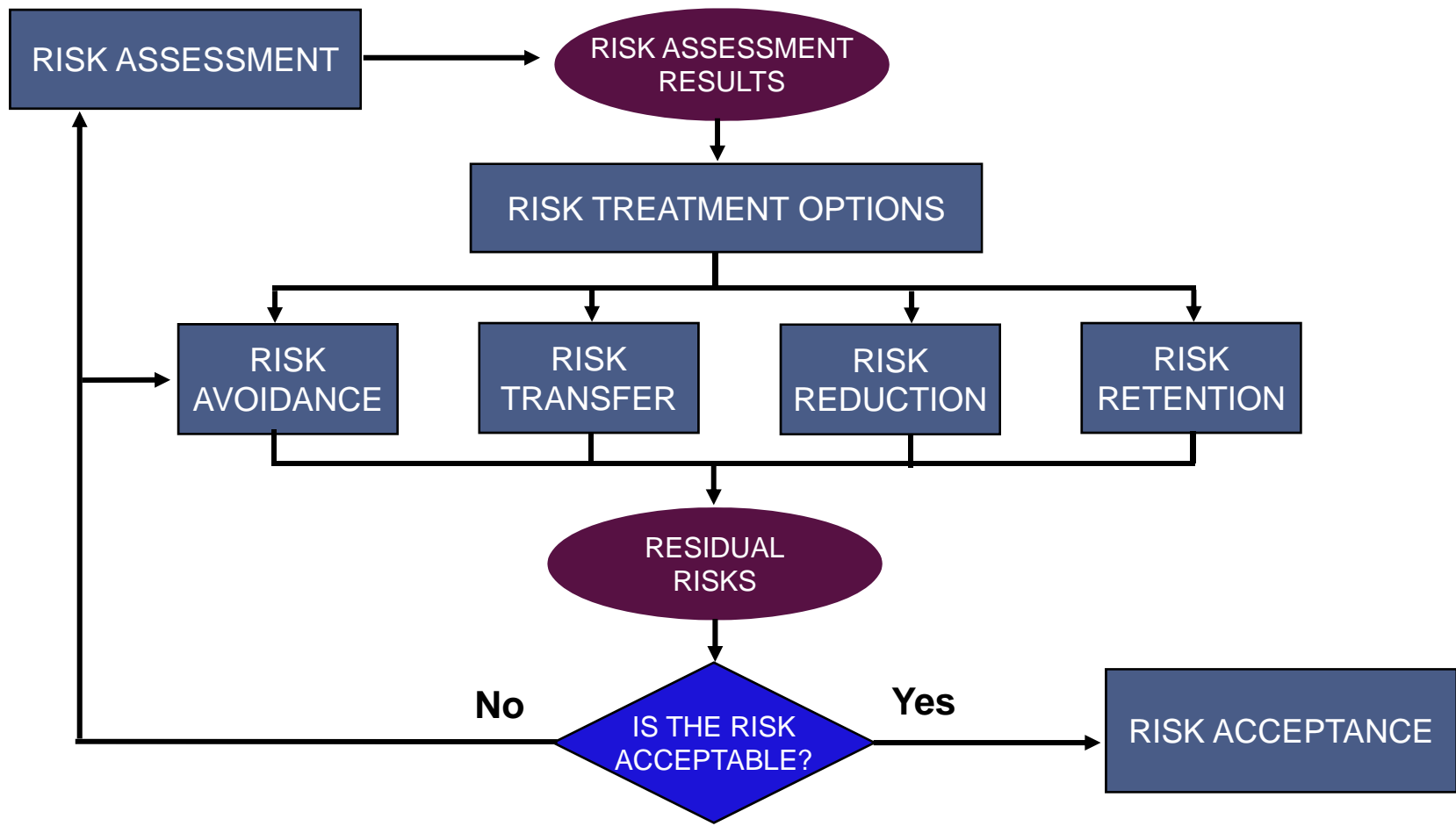
## ➤ How reliable are the records:

- ◆ Complete?
- ◆ Accurate?
- ◆ Have not been modified or tampered?

## ➤ You need to be able to prove individual accountability and be able to support investigation of incidents

# Risk Mitigation

# Risk Treatment Decision-making Process



**BASED ON:** ISO/IEC 27005:2008, *Information technology -- Security techniques – Information Security Risk Management*, <http://www.iso.ch>

# Compensating Controls

- A compensating control is a way of mitigating a known risk where it may not be feasible to deploy specific technical enablement
- Considerations for compensating controls:
  - ◆ Demonstrate that a risk analysis has been performed
  - ◆ Document the constraints- technical or business
  - ◆ After the implementation be able to demonstrate the effectiveness has been evaluated
  - ◆ Longevity and review frequency

# Compensating control example

- PCI 3.6.6 Split knowledge and establishment of dual control of keys (requiring two or more people, each knowing only a part of the key, to reconstruct the entire key)
  - ◆ Could be implemented in a product supporting smart cards, or other quorums
  - ◆ Or the compensating control could be:
    - › Physically isolated key storage
    - › Requiring two people with different keys to authorize the unlocking of key storage
    - › Rigid documentation of key access and the security of both the keys themselves and the key storage itself

# What Data Do You Really Need?

- Who has responsibility for and makes changes in the storage environment
  - ◆ Servers
    - > HBAs, volume managers, NFS or Windows file sharing
  - ◆ Fabric
    - > Physical and logical access
  - ◆ Switches
    - > Physical and logical access
    - > zoning
  - ◆ Storage
    - > LUN masking
    - > Storage provisioning
    - > upgrade/replacement
    - > Handling of physical media
- Best Practices
  - ◆ Ensure there are no default or common user ids for making changes

# Audit logs

## ➤ Aggregation

- ◆ Enable logging on all devices
- ◆ Collect logs
- ◆ Correlate
- ◆ Retain

## ➤ Analysis

- ◆ Access and change control audits

## ➤ Alerting

- ◆ Is there a mechanism for triggering action when something may be wrong

## ➤ Archiving

- ◆ Including using secure hashes to maintain integrity

# What Other Capabilities Should You Consider?

- Don't ignore the replicated and backup data
  - ◆ The data may not be in production – but it could still be a source for leakage or retention requirements
  - ◆ In general requires similar treatment to live data
- Don't forget remote or Disaster Recovery sites
  - ◆ Eliminate confusion about how these sites are treated
- Be explicit about the use of 3<sup>rd</sup> party service providers
  - ◆ Have documentation for the service level agreements you have in place and pointers for any compliance documentation they may have available

- There may still be gaps after deployment of technology
  - ◆ Risk assessments may be required both before and after deployment to be able to identify gaps
- Remember that controls can be:
  - ◆ Physical
  - ◆ Administrative
  - ◆ Technological
- Depending on specific requirements and the outcome of an assessment, it is also sometimes possible to accept all or partial risk

# Other Sources of Helpful Information

- A source for the storage security best practices is:  
[http://www.snia.org/forums/ssif/programs/best\\_practices](http://www.snia.org/forums/ssif/programs/best_practices)
  
- 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

- The SSIF works together on a variety of exciting projects
  - ◆ Publishing Solutions Guides, white papers and articles on storage security
  - ◆ Creating SSIF educational materials and SNIA Education Storage Security Tutorials
  - ◆ Educating end users and colleagues as speakers in security and storage events
  - ◆ Contributing to storage security Best Current Practices
- SSIF Membership is open to storage, security, and audit professionals and their companies
- Building a community where members work together to contribute to a better understanding of storage security and how it applies in the organization.

*SSIF – Where Storage and Security Meet*

# Reference Links

- ▶ Link to processes, policies, and procedures (overview) that should be documented for a HIPAA audit:  
<http://www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsTechnicalSafeguards.pdf>
- ▶ The main website has a lot of useful information too:  
<http://www.cms.hhs.gov>
- ▶ For HIPAA security audits:  
[http://www.training-hipaa.net/compliance/Official-HIPAA-Security-Compliance-Audit-checklist\\_document-by-DHHS.pdf](http://www.training-hipaa.net/compliance/Official-HIPAA-Security-Compliance-Audit-checklist_document-by-DHHS.pdf)

## PCI-DSS security audits:

[https://www.pcisecuritystandards.org/pdfs/pci\\_audit\\_procedures\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf)

# Summary

- Know what may be required from you during and after a security audit
  - ◆ Review storage security best practices and have a plan for improvement
- What data collection should you be doing to be prepared for an audit
  - ◆ Documentation of procedures, practices, change control, audit logs
- What procedures and processes should you be implementing to make the audit go smoothly
  - ◆ Be Proactive!
- What are the capabilities and solutions you should look for to help in producing the materials required by an audit
  - ◆ Administration authentication, role based access control
  - ◆ Audit log capabilities such as ability to sign and ship off the box

- 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**

**Blair Semple, CISSP  
Phil Huml  
Gordon Arnold**

**Eric Hibbard, CISSP  
Andrew Neilsen, CISSP  
Larry Hofer**