Storage Security Best Practices

Eric A. Hibbard, CISSP, CISA / Hitachi Data Systems

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.

Abstract

Storage Security Best Practices

Many organizations face the challenge of implementing protection and data security measures to meet a wide range of requirements, including statutory and regulatory compliance. Often the security associated with storage systems and infrastructure has been missed because of limited familiarity with the storage security technologies and/or a limited understanding of the inherent risks to storage ecosystems. The net result of this situation is that digital assets are needlessly placed at risk of compromise due to data breaches, intentional corruption, being held hostage, or other malicious events.

Both SNIA and ISO/IEC are combating this situation by providing materials that can be used to address storage security issues. In the case of ISO/IEC, the materials are contained in a new International Standard that seeks to provide detailed technical guidance on the protection (security) of information where it is stored and to the security of the information being transferred across the communication links; it includes the security of devices and media, the security of management activities related to the devices and media, the security of applications and services, and security relevant to end-users.

Outline

- **Storage Security 101**
- Major Storage Threats & Challenges
- Prevailing Storage Security Guidance
- Storage Security Standardization
- Summary

What is Storage Security?

- application of physical, technical and administrative controls to protect storage systems and infrastructure as well as the data stored within them

  Note 1 to entry: Storage security is focused on protecting data (and its storage infrastructure) against unauthorized disclosure, modification or destruction while assuring its availability to authorized users.

  Note 2 to entry: These controls may be preventive, detective, corrective, deterrent, recovery or compensatory in nature.

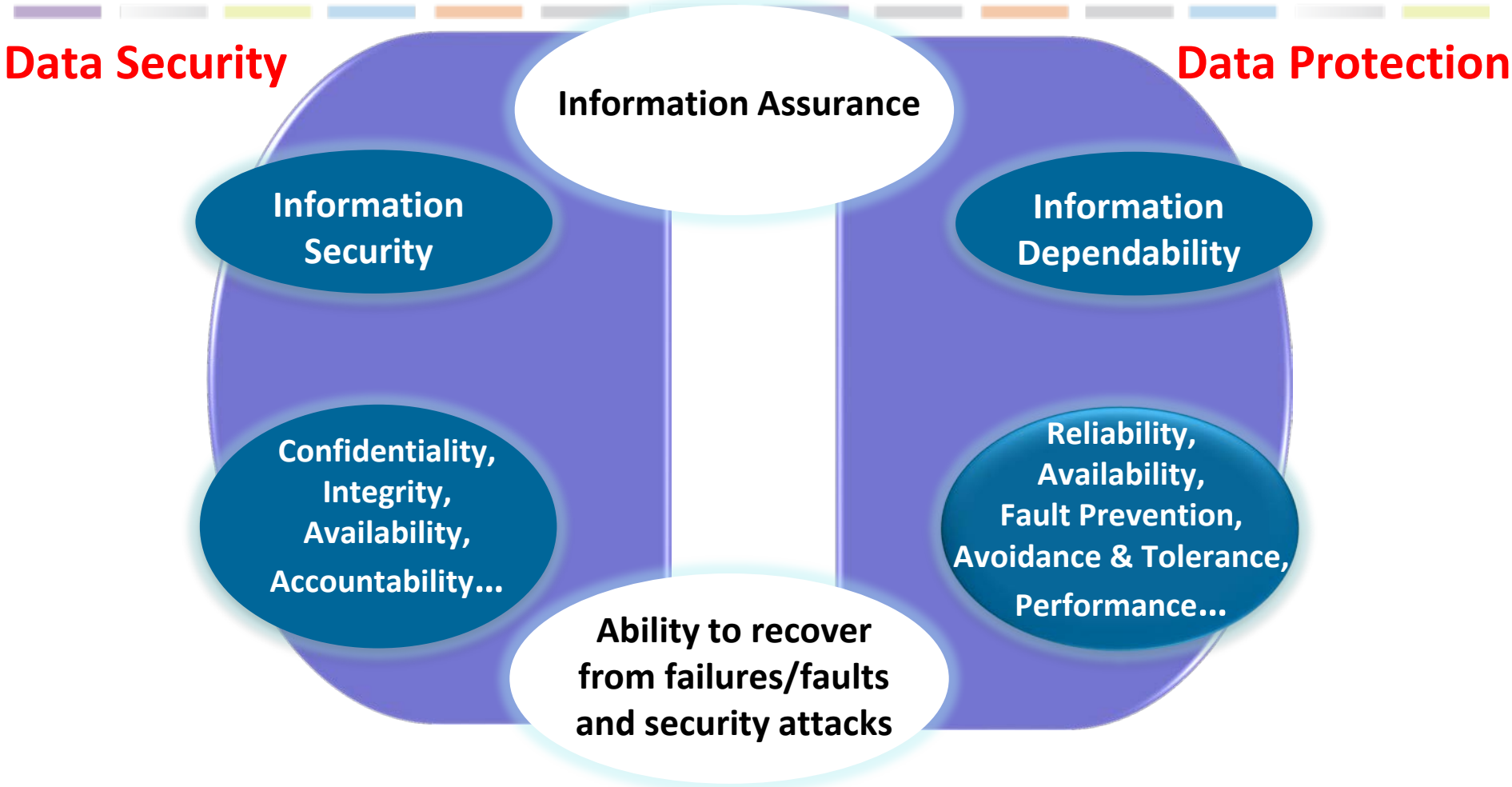
  – ISO/IEC 27040:2015

- Technical controls, which may include integrity, confidentiality and availability controls, that protect storage resources and data from unauthorized users and uses.

  – SNIA Dictionary

- Simply a part of ***Information Assurance***

Information Security & Dependability

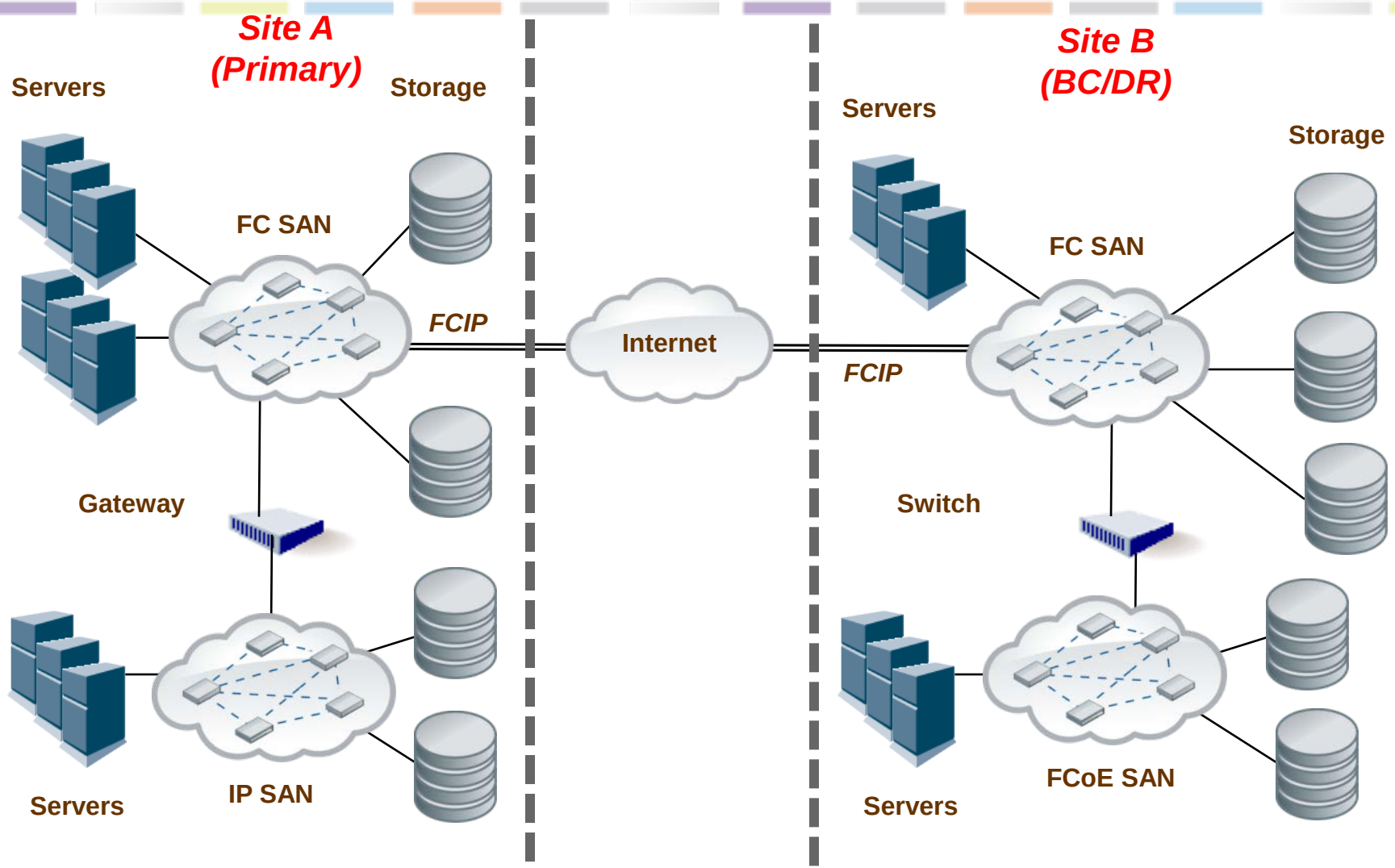


SOURCE: *Information Assurance – Dependability and Security in Networked Systems*, Qian, Joshi, Tipper, Krishnamurthy, 2008, New York, ISBN: 978-0-12-373566-9.

Business Drivers for Data Security

- Theft Prevention
- Prevention of Unauthorized Disclosure
- Prevention of Data Tampering
- Prevention of Accidental Corruption/Destruction
- Accountability
- Authenticity
- Verifiable Transactions
- Business Continuity
- Regulatory and Legal Compliance

Sample Storage Ecosystem



Outline

- Storage Security 101
- **Major Storage Threats & Challenges**
- Prevailing Storage Security Guidance
- Storage Security Standardization
- Summary

Threat Agents

External

- Nation States
- Hackers
- Terrorists/Cyberterrorists
- Organized Crime
- Other Criminal Elements
- International Press
- Industrial Competitors

Internal

- Careless Employees
- Poorly Trained Employees
- Disgruntled Employees
- Partners

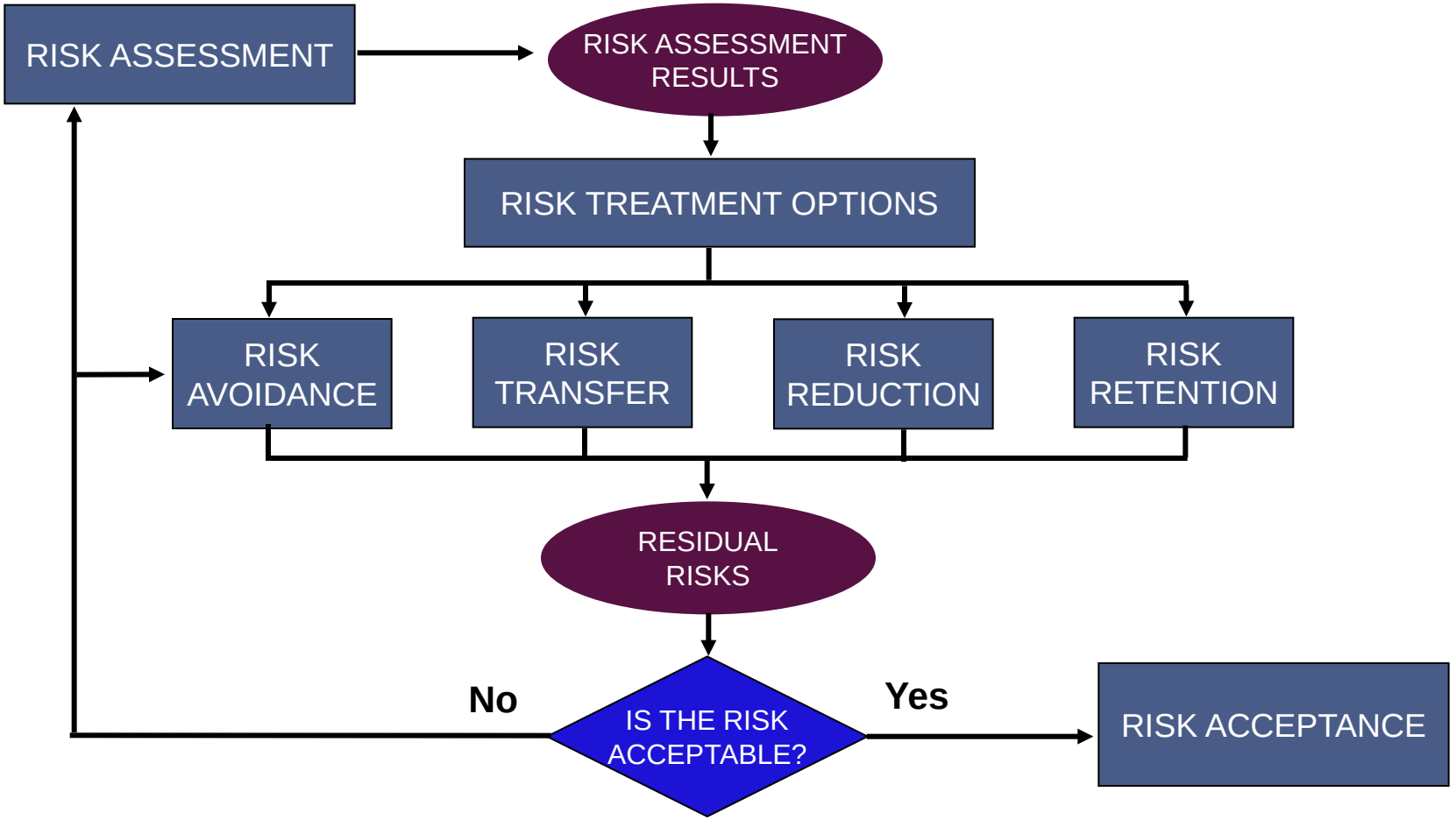
Major Threats to Storage

- Unauthorized usage
- Unauthorized access
- Liability due to regulatory non-compliance
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks on storage
- Corruption/modification and destruction of data
- Data leakage/breaches
- Theft or accidental loss of media
- Malware attack or introduction
- Improper treatment or sanitization after end-of-use

Other Threats

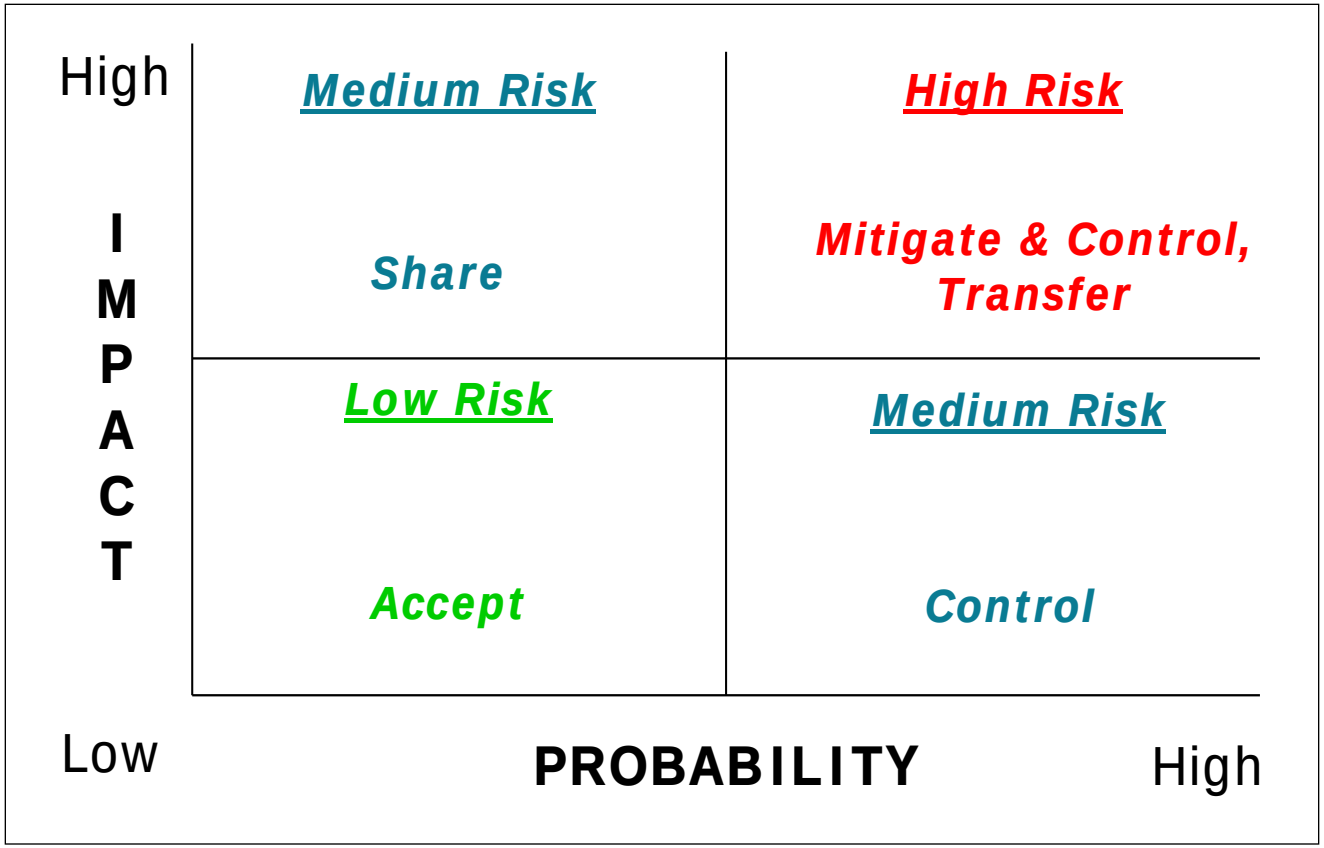
- Data Corruption or Destruction
  - Unintentional – fire, flood, power outages, programming bugs and user errors
  - Intentional
    - Attacks/events of a malicious nature can be perpetrated by external parties and/or insiders with the purpose of making some or all of the affected data unusable or destroyed
    - Non-malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as “getting the job done"
- Temporary or permanent loss of access/availability
- Failure to meet statutory, regulatory, or legal requirements

Risk Treatment Decision-making Process



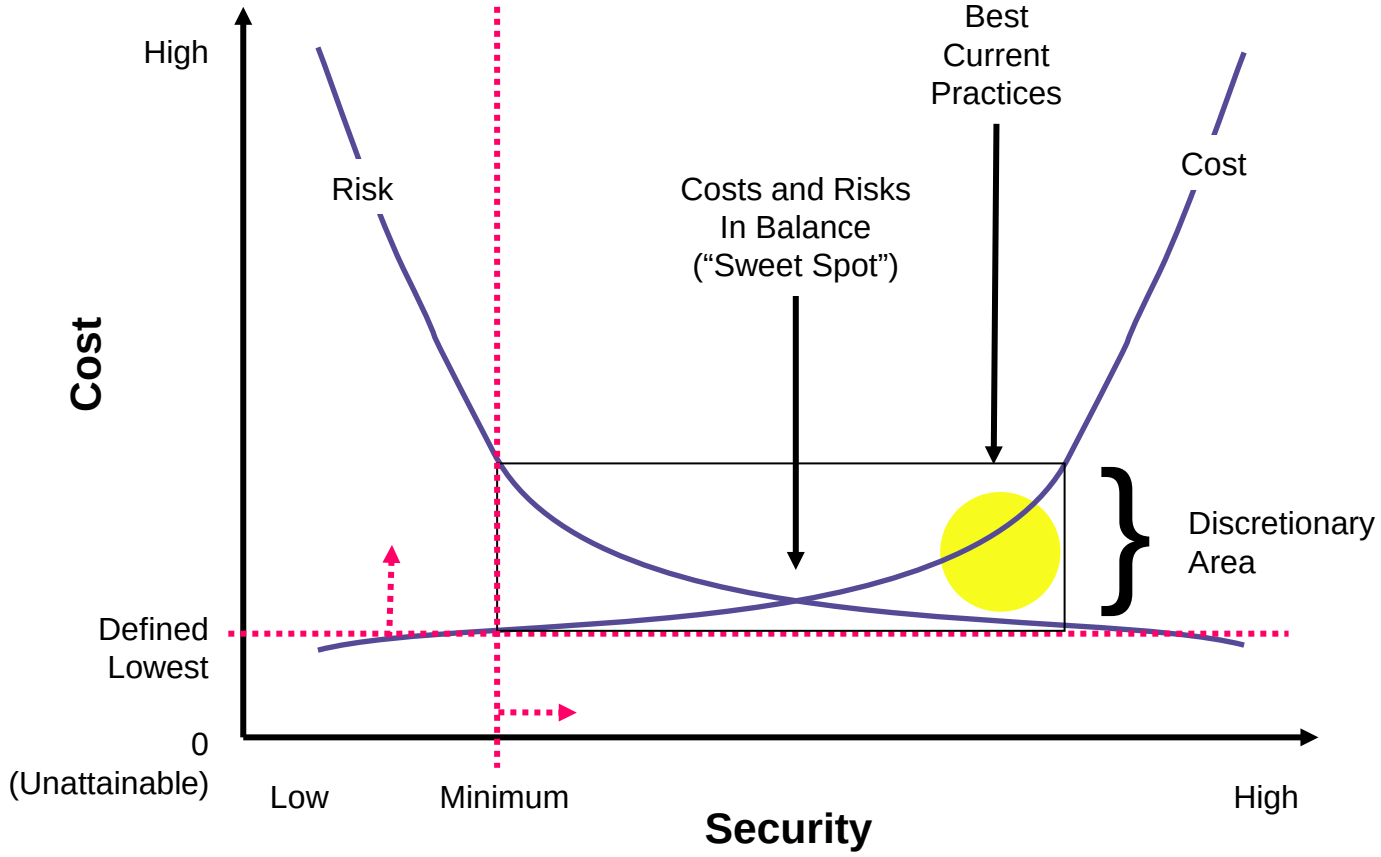
SOURCE: ISO/IEC 27005:2008, *Information technology -- Security techniques – Information Security Risk Management*, http://www.iso.ch

Risk and Remediation



A simple way of identifying the highest priority risks as well as offering some guidance on what should be done.

Balancing Cost & Security



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

Outline

- Storage Security 101
- Major Storage Threats & Challenges
- **Prevailing Storage Security Guidance**
- Storage Security Standardization
- Summary

Balance Security and Compliance

Data Security	Compliance
Proactive	Reactive
Defense-in-depth	Accountability
Physical, technical and administrative control areas	Traceability
Preventive, detective and corrective control types	Monitoring & Reporting
	Risk Management
	Often the driver for security

Policy & Planning

- Incorporate storage into policies
  - Identify most sensitive and business critical data categories as well as protection requirements
  - Integrate storage-specific policies with other policies where possible
  - Address data retention and protection
  - Address data destruction and media sanitization
- Ensure conformance with policies
  - Ensure that all elements of the storage ecosystem comply with policy
  - Prioritize activities based on the sensitivity/criticality of the data
- Review the policies and plans
  - Align process with policy
  - Create a data retention plan
  - Create an Incident Response Plan
- Identify technology & data assets; do a basic classification
- Make sure storage participates in the continuity measures

User Controls

- Focus on user authentication and access controls
  - Changing default credentials is key
  - Avoid shared credentials
  - Perform regular user account (entitlement) reviews
  - Factor in human resources (HR) termination procedures
- Secure business partner connections
- Profile expected/normal transactions and traffic
  - Look for things that are “anomalous” or “suspicious”
  - Include time and dates as part of the profile
- Implement monitoring and reporting
  - Enable application logs as well as systems logs
  - Accountability and traceability (logging and access controls)

Use Risk Domains

- Control data with transaction zones
  - Base on data discovery and classification
  - Implement risk-based separation and enhanced controls
- Use risk domains to limit access and damage
- Protect the management interfaces from unauthorized access and reconnaissance
- Ensure that backups and replication don’t become a source of unauthorized data access or disclosure

Implement Essential Controls

- Achieve essential, and then worry about excellent
  - Identify essential controls
  - Implementation across the organization without exception
  - Employ smarter patch management strategies
- Understand the security posture of your storage systems/ecosystems and adjust appropriately
- Implement appropriate data protections (out-of-area disaster recovery, retention, WORM, archive)
- Sanitize media (overwriting or cryptographic) used to store sensitive data

Outline

- Storage Security 101
- Major Storage Threats & Challenges
- Prevailing Storage Security Guidance
- **Storage Security Standardization**
- Summary

Introduction to ISO/IEC 27040:2015

- Common set of guidance for security and storage professionals
- Primary perspective is for customers, but it also addresses vendor issues
- For storage systems and ecosystems, it addresses
  - the physical, technical and administrative controls
  - the preventive, detective and corrective controls
- Covers concepts, technology-specific controls, and design/implementation guidance
- Definitive standard for data/media sanitization
- Storage security checklists (for auditors)
- Available: http://www.iso.org (CHF 198)

ISO/IEC 27040 – Concepts

- Defines important terminology
- Introduces storage concepts (for security personnel)
- Introduces storage security concepts
- Identifies the real and perceived risks
- Describes important security concepts (Annex C)
  - Authentication, authorization, and access control
  - Self-encrypting drives
  - Sanitization
  - Logging
  - N_Port_ID Virtualization (NPIV)
  - Fibre Channel security
  - OASIS KMIP

ISO/IEC 27040 – Data Breaches

Security threats	Potential forms of data breach
Theft of storage element or media	Unlawful access, unlawful disclosure, unlawful data loss, unlawful data destruction
Loss of storage element or media	Unauthorized access, unauthorized disclosure, accidental data loss, accidental data destruction
Loss of data	Unlawful, unauthorized, or accidental data destruction or corruption
Accidental configuration changes (e.g., storage management, storage/network resources, incorrect patch management, etc.) by authorized personnel	Accidental access, accidental disclosure, accidental data destruction, accidental data alteration
Malicious configuration changes (storage management, storage/network resources, application tampering, etc.) by external or internal adversaries	Unlawful access, unlawful disclosure, unlawful data destruction, unlawful data alteration
Privileged user abuses by authorized users (e.g., inappropriate data snooping)	Unlawful/unauthorized access or disclosure
Malicious data tampering by external or internal adversaries	Unlawful data destruction or alteration
Denial of service attacks	Unauthorized data destruction, loss, or alteration
Malicious monitoring of network traffic	Unlawful/unauthorized disclosure

ISO/IEC 27040 – Technology Controls

- Controls that *support* storage security technical architectures, their related technical controls, and other controls (technical and non-technical) that are applicable not just to storage
- Technology controls organized by
  - Direct Attached Storage
  - Storage Networking (SAN & NAS)
  - Storage Management
  - Block-based Storage (Fibre Channel & IP)
  - File-based Storage (NFS and SMB/CIFS)
  - Object-based Storage (cloud storage, OSD & CAS)
  - Storage Security Services (sanitization, confidentiality, data reductions)

ISO/IEC 27040 – Design/Implementation

- Technology controls and guidance have to be integrated into the design and implementation of storage security solutions to counter storage security threats
- Design and implementation guidance organized by
  - Storage Security Design Principles
  - Data Reliability, Availability, and Resilience
  - Data Retention (short and long-term archives)
  - Data Confidentiality and Integrity
  - Virtualization
  - Design and Implementation Considerations (encryption, policy, compliance, secure multi-tenancy, and secure autonomous data movement)

Hidden Nuggets

- *Cloud Storage* – Generic guidance as well as specific guidance for CDMI
- *Secure Multi-tenancy* – General characterization as well as how it applied to storage
- *Secure Autonomous Data Movement* – ILM Security Reincarnated
- *Data/Media Sanitization (Annex A)*
  - Aligned with NIST SP 800-88r1 (Media Sanitization)
  - **Cryptographic Erase** – New form of sanitization
  - Can be "referenced" like DoD 5222.20-M (1995)
- *Checklists* – Selecting storage security controls (Annex B)
- *Bibliography* – One of the few comprehensive lists covering all the pieces and parts of storage security

Selecting Storage Security Controls (1)

- Provides information to assist in making phasing or sequencing decisions for control implementation (over 330 controls)
- Data sensitivity classes
  - Provides a data-centric focus that leverages two classes: Low (L) and High (H); applicability is identified with an "X"
  - Can be used by organizations that have performed basic data classifications
- Security priority codes
  - Based on the relative importance of the confidentiality (C), integrity (I), and availability (A) aspects of security
  - Values are in the range of 0 to 5, with 5 representing the highest priority and 0 is the lowest priority;

Selecting Storage Security Controls (2)

Table B.1 — Direct Attached Storage (Subclause 6.2)

Controls	Priorities (5 is highest)				Data Sensitivity	
	S	C	I	A	L	H
DAS should be physically secured		5	3	5	X	X
For sensitive and high value data on DAS, some form of encryption (SED, FDE, host-based, or application-based) should be used to protect the data at rest		5	3	0		X
Media sanitization should be used on all DAS involved with sensitive and high value data		5	1	0		X
If possible, authentication (e.g., FC-SP Authentication) should be used to prevent unauthorized access to sensitive and high value data		5	3	0		X
To guard against accidental or intentional data loss or corruption, backups of the DAS contents should be made on a regular basis		0	5	0	X	X

NOTE: All of the 27040 controls are summarized in Annex B.

Exploiting ISO/IEC 27040

- Customer Perspective
  - Internationally recognized guidance
  - Can be an important reference for RFPs for storage products and service contracts (guidance can be turned into requirements)
- Vendor Perspective
  - Major threats and risks identified
  - Insight into how technology-specific controls fit into an overall storage security approach

- Although a *guidance* standard, ISO/IEC 27040 could easily become a source of *requirements*, which introduce compliance issues.

Raising the Security Bar for Storage

- The sheer existence of ISO/IEC 27040 is causing the security community to take note of the security needs and posture of storage infrastructure
- ISO/IEC 27040 will help identify other important and related standards and specifications (e.g., FC-SP)
- Specific criteria (like media sanitization methods) will be documented in a way that they can be used by both vendors and customers
- ***BOTTOM LINE:*** ISO/IEC 27040 will define best practices that ultimately set the minimum expectations for storage security.

SNIA and ISO/IEC 27040

- SNIA was an early source of storage security guidance
- Comments and significant contributions were provided to ISO/IEC JTC 1/SC 27 (via INCITS/CS1 and Cloud Security Alliance)
- Serving as the primary champion of the standard
  - http://www.snia.org/securitytwg
  - Developed a detailed “index” for the standard
- Value-added materials under development
  - Sanitization whitepaper
  - Encryption and key management whitepaper
  - Data protection whitepaper
  - Refresh of *Professionals Guide to Storage Security*

Outline

- Storage Security 101
- Major Storage Threats & Challenges
- Prevailing Storage Security Guidance
- Storage Security Standardization
- **Summary**

The Landscape

- Due to the increased activities of organized crime groups and government entities, external threats are a more likely source of data breaches
- The attackers are adapting to our current protection strategies and inventing new ways to attain the data they value.
- A significant number of breaches can be avoided if simple or intermediate security controls are in place at the time of the incident.

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!

- Protect critical/sensitive/regulated data when it leaves your control
- ***Manage*** the risks or ***suffer*** the consequences
- Have a plan to deal with data security incidents

- Consider…It is not a matter of ***IF*** you will be attacked, but rather ***WHEN*** and if you will ***KNOW*** that you have been attacked.

SNIA Security Organizations

- SNIA Security Technical Work Group (TWG)
  - Focus: Requirements, architectures, interfaces, practices, technology, educational materials, and terminology for storage networking.
- Storage Security Industry Forum (SSIF)
  - Focus: Educational materials, customer needs, whitepapers, and best practices for storage security.
- http://www.snia.org/security

Attribution & Feedback

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

Authorship History

Eric Hibbard, CISSP, CISA (Spring 2014)

(incorporating materials from earlier tutorial dating back to 2010)

Updates:
Eric Hibbard, CISSP, CISA (March 2015)

Additional Contributors

SNIA Security TWG

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