Education

Introduction to Storage Security

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

SNIA Legal Notice

- 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.

Abstract

Introduction to Storage Security

As society becomes more dependent on IT and digital assets, the social impact of the failure of IT resources ceases to be an inconvenience and begins to take on the character of a disaster. Few other elements of the IT infrastructure have a more important relationship with data than that of storage systems. They may also be the last line of defense against an adversary, but only if storage managers and administrators invest the time and effort to implement and activate the available storage security controls.

This session covers the storage security fundamentals. It starts by providing information on the types of data that should be protected along with the drivers for this protection. Next, it summarizes important information assurance and security concepts, with a particular emphasis on risk. It continues with a characterization of storage security and concludes with practical guidance on starting a storage security program.

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

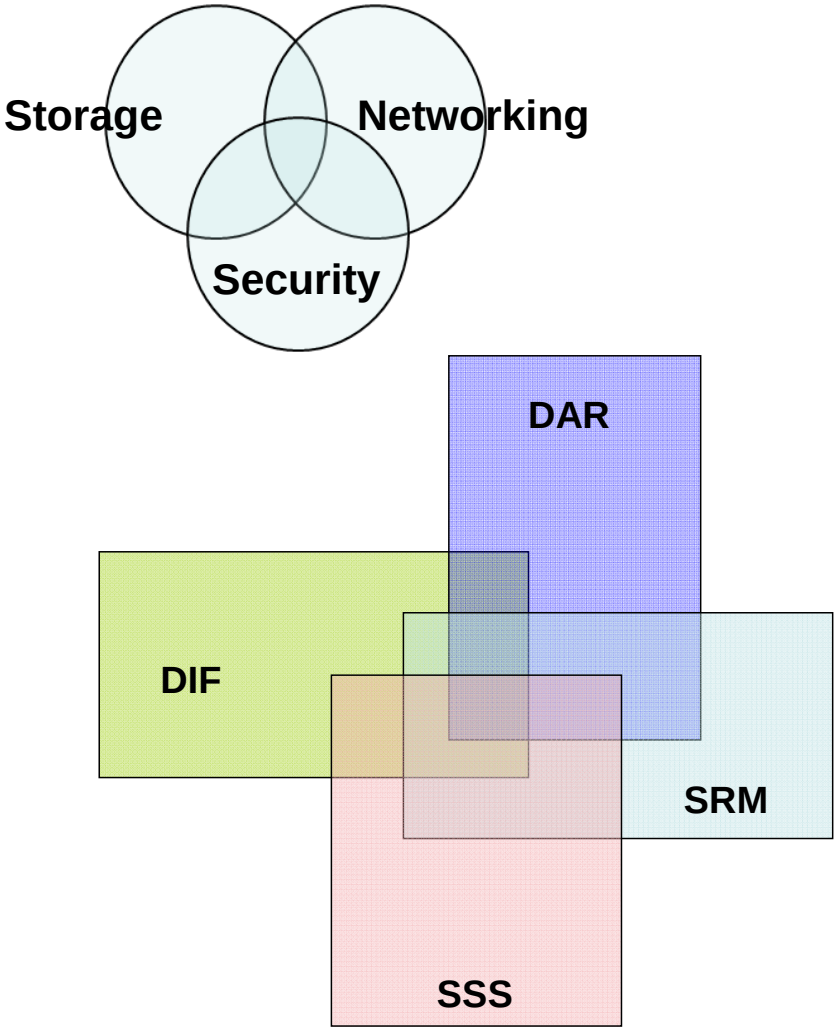
- ***Convergence*** of the storage, networking, and security.

- Simply a part of ***Information Assurance***
  - Measures that protect and defend information and systems
  - Encompasses system reliability and strategic risk management
  - Provides for restoration of information systems using protection, detection, and reaction capabilities

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

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).

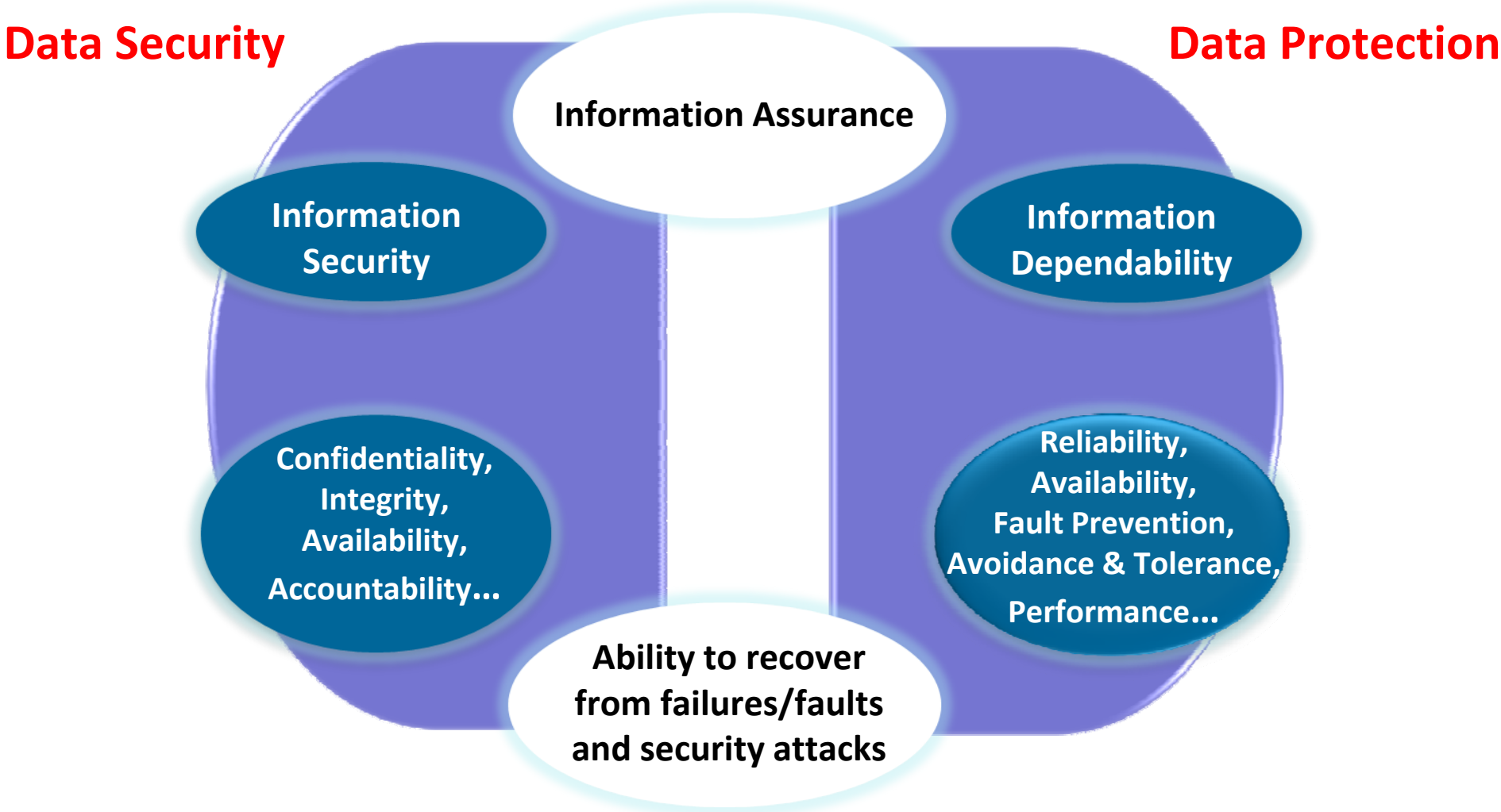
It's All About the Data

- Types of sensitive and valuable data:
  - personal, private information (including personally identifiable information or PII)
  - business information
  - national security (both classified and unclassified) information
- One should generally protect data:
  - that is worthy of protection,
  - in proportional to its value, and
  - only for its useful lifetime.
- Use a few data security classification categories to keep the classification process manageable
  - Focus on most sensitive, valuable and/or critical

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

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.

IA Core Principles

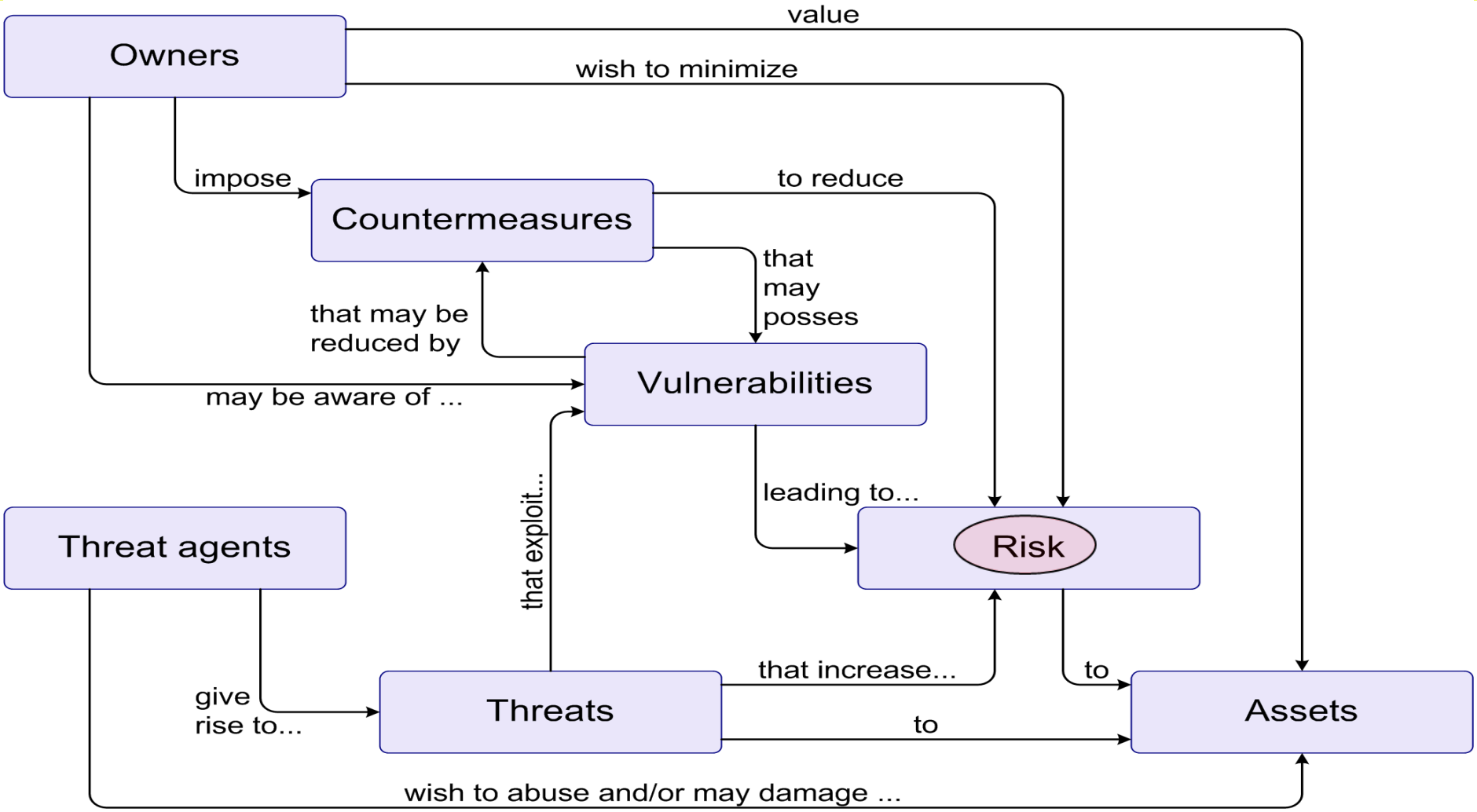
- **Confidentiality** – ensures the disclosure of information only to those persons with authority to see it.
- **Integrity** – ensures that information remains in its original form; information remains true to the creators intent
- **Availability** – information or information resource is ready for use within stated operational parameters
- **Possession** – information or information resource remains in the custody of authorized personnel
- **Authenticity** – information or information resources conforms to reality; it is not misrepresented as something it is not

IA Core Principles (cont.)

- **Utility** – information is fit for a purpose and in a usable state
- **Privacy** – ensures the protection of personal information from observation or intrusion as well as adherence to relevant privacy compliances
- **Authorized Use** – ensures cost-incurring services are available only to authorized personnel
- **Nonrepudiation** – ensures the originator of a message or transaction may not later deny action

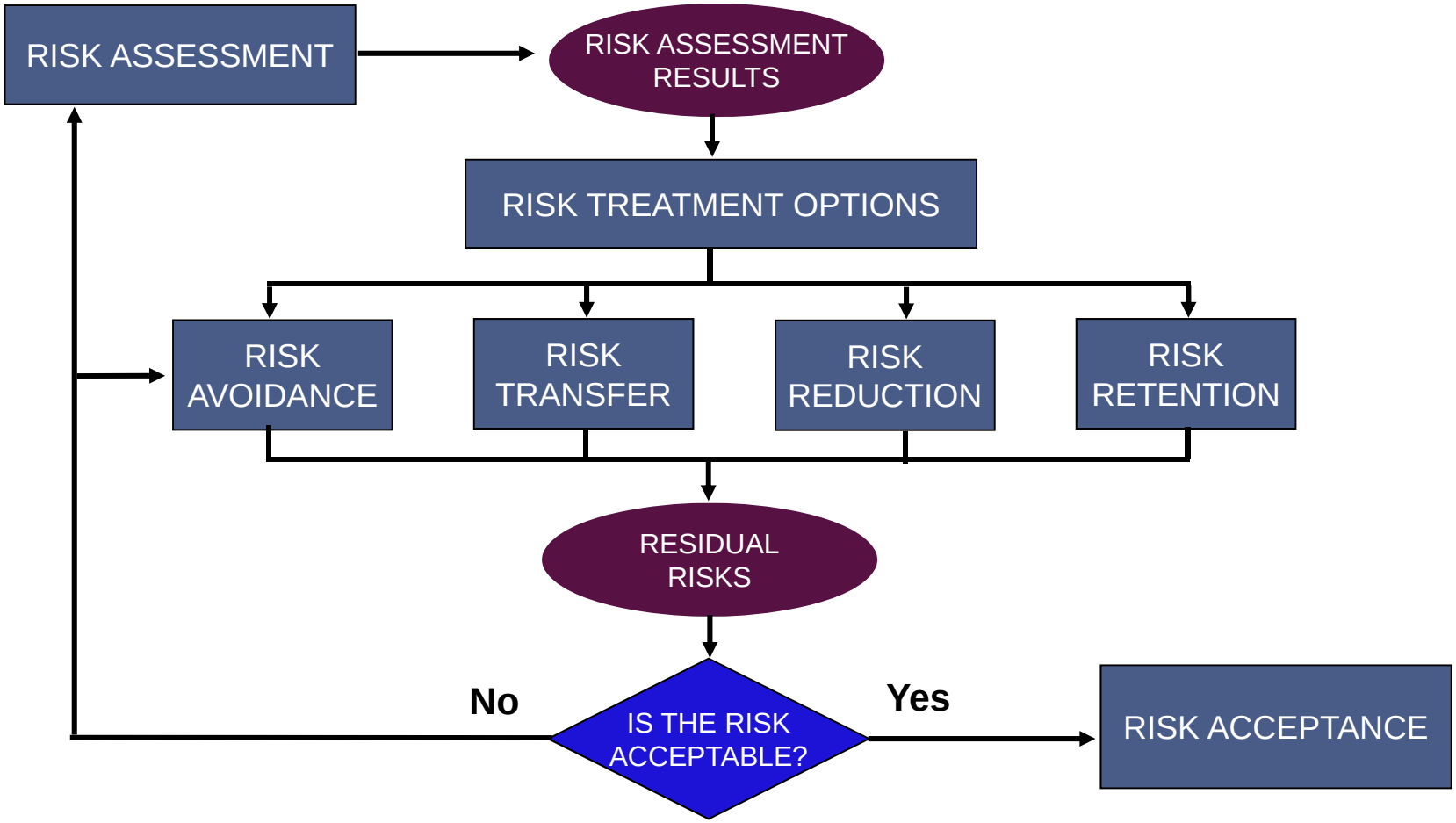
NOTE: These IA Principles are based on the Parkerian Hexad model.

The Security "Big Picture"



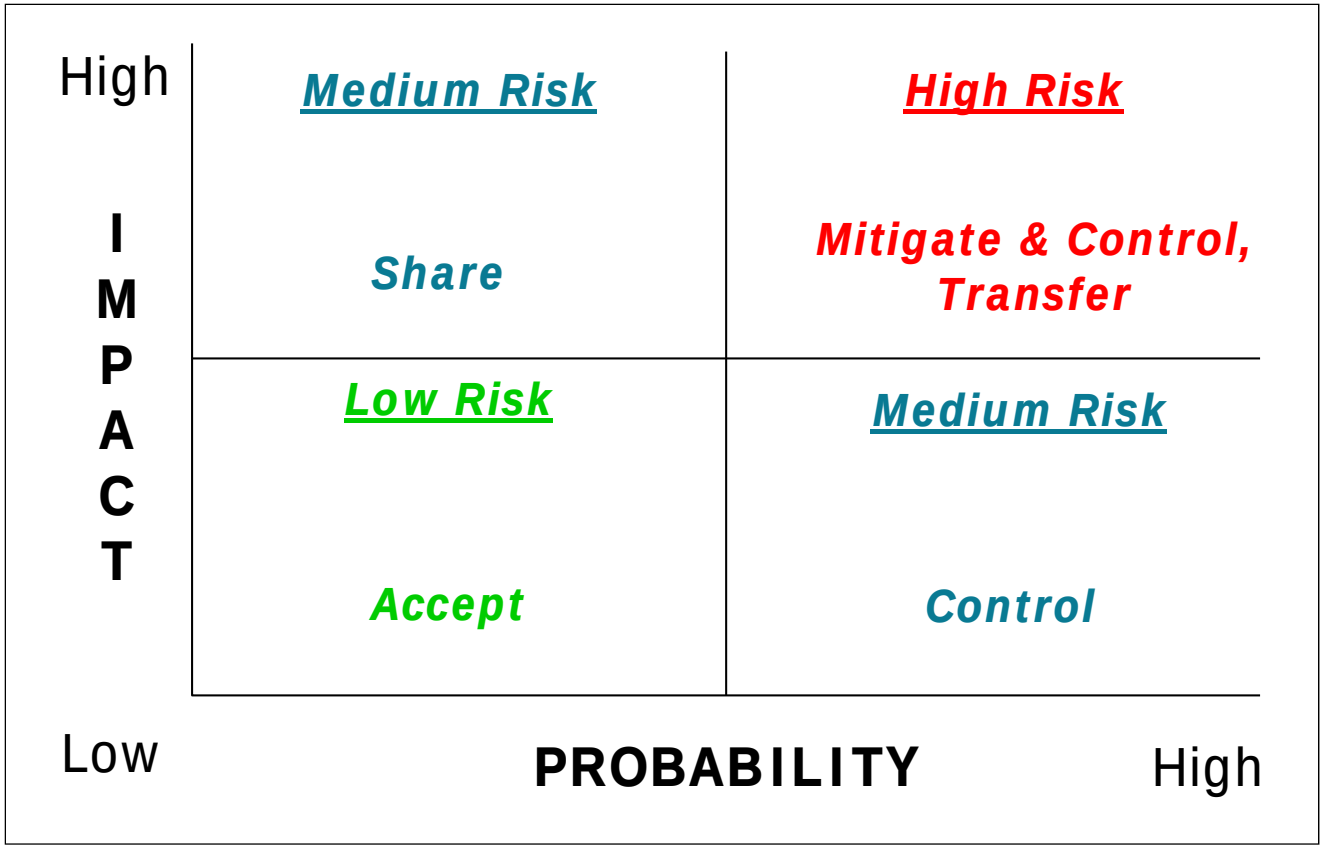
SOURCE: ISO/IEC 15408-1:2009, *Information technology -- Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*, http://www.iso.ch

Risk Treatment Decision-making Process



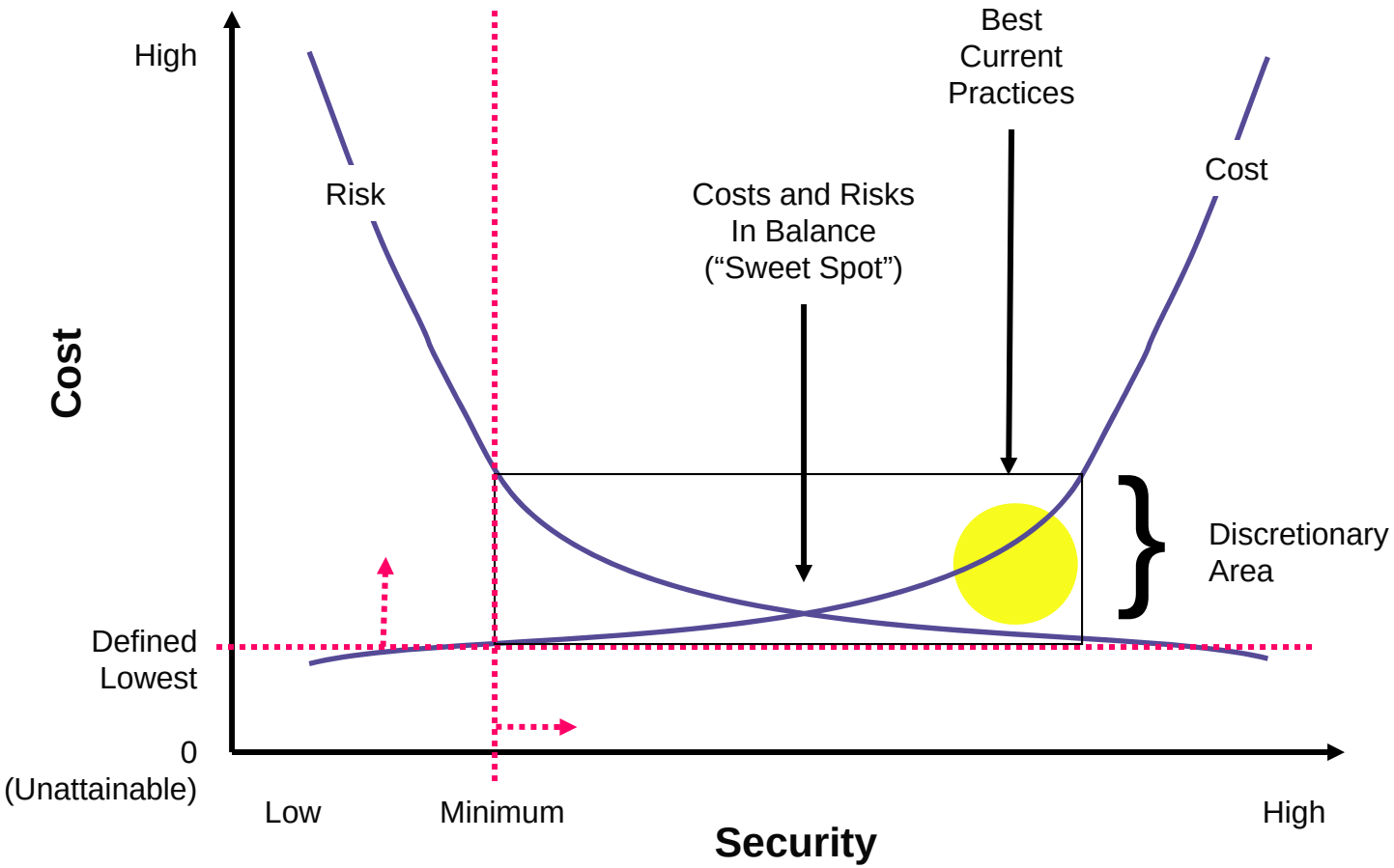
SOURCE: ISO/IEC 27005:2008, *Information technology -- Security techniques – Information Security Risk Management*, http://www.iso.ch

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.

Common "Security" Frameworks

- ISO/IEC 27002:2005 *The Code of Practice for Information Security Management* & ISO/IEC 27001:2006 *Information Security Management - Requirements*
- IT Governance Institute (ITGI), Control Objectives for Information and related Technology (COBIT) Version 4.1
- 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

Security Challenges for Storage Ecosystem

- Control of Privileged Users (Administrators)
- Protection of Storage Management
- Credential & Trust Management
- Data In Flight Protection
- Data At Rest Protection
- Data Availability Protection (redundancy, resiliency, integrity, performance)
- Data Backup & Recovery (disaster recovery, business continuity)
- Defense & Intelligence (labeled storage, MLS)
- Information Lifecycle Management (ILM)

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

Anatomy of Data Breaches

(2009 Data Breach Investigations Report)

- What commonalities exist?
  - 69% were discovered by a third party
  - 81% of victims were not PCI DSS compliant
  - 83% of attacks were not highly difficult
  - 87% were considered avoidable through simple or intermediate controls
  - 99.9% of records were compromised from servers and applications
- Who is behind data breaches?
  - 74% resulted from external sources
  - 20% were caused by insiders
  - 32% implicated business partners
  - 39% involved multiple parties

91% of all compromised records were linked to organized criminal groups.

Anatomy of Data Breaches

(2009 Data Breach Investigations Report)

- Threat categories (% breaches / % records)
  - Hacking 64% / 94%
  - Malware 38% / 90%
  - Misuse 22% / 2%
  - Deceit 12% / 6%
  - Physical 9% / 2%
  - Error (cause) 1% / 0%
  - Environmental 0% / 0%

- How do data breaches occur?
  - 67% were aided by significant errors
  - 64% resulted from hacking
  - 38% used malware
  - 22% involved privilege misuse
  - 9% occurred via physical attacks

17% of attacks were designated to be highly difficult, yet they accounted for 95% of the total records breached.

"Hacking gets the criminal in the door, but malware gets him the data."

Storage Security Guidance
(A Place to Start)

Check out SNIA Tutorial:

Active Archive - Data Protection for the Modern Data Center

SOURCE: SNIA Technical Proposal, *Introduction to Storage Security, v2.0*, © 2009, http://www.snia.org/forums/ssif/knowledge_center/white_papers/

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
  - Define "suspicious" and "anomalous" and then look for whatever "it" is
  - Enable application logs as well as systems logs
- Implement monitoring and reporting
  - 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

Final Thoughts

Balance Security and Compliance

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

- Due to the increased activities of organized crime groups and government entities, external threats are a more likely source of data breaches
- A significant number of breaches can be avoided if simple or intermediate security controls are in place at the time of the incident.
- 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

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!
- The attackers are adapting to our current protection strategies and inventing new ways to attain the data they value.
- It is not a matter of *IF* you will be attacked, but rather *WHEN* and if you will *KNOW* that you have been attacked.

Q&A / Feedback

- 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, PE
Roger Cummings
Tim Smith
Richard Austin, CISSP
Andrew Nielsen, CISSP, CISA
Ray Kaplan, CISSP
Gianna DaGiau

SNIA Security TWG

For More Information

SNIA Security Materials

- Storage Networking Industry Association, Technical Proposal, *Storage Security Best Current Practices (BCPs) v2.1.0*, http://www.snia.org/forums/ssif/programs/best_practices/
- Storage Networking Industry Association, *Introduction to Storage Security – Version 2.0*, 2009, http://www.snia.org/forums/ssif/
- Storage Networking Industry Association, *Storage Security: The SNIA Technical Tutorial*, 2004, http://www.snia.org/education/storage_networking_primer/storage_security/
- Storage Networking Industry Association, *Storage Security Professional's Guide to Skills and Knowledge – Version 1.0*, 2008, http://www.snia.org/forums/ssif/

SNIA Security Organizations

- 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: Educational materials, customer needs, whitepapers, and best practices for storage security.
  - http://www.snia.org/ssif