SNIA

STORAGE NETWORKING INDUSTRY ASSOCIATION

EDUCATION

A Chief Information Security Officer's (CISO) View of Storage Security

Eric Hibbard, CISSP, CISA

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.

Tutorial Abstract

The CISO is accountable for the mitigation of risk. Their diligence assures the success of their organization. While securing the storage in all of its forms may be tasks of the storage team, if that team fails, the CISO may pay the price. C-Level Security Executives are leaders who set vision, choose information security models, define the security services, build a team, manage budget, run the business and prepare for potential crises all for one purpose: to meet business and regulatory expectations. To understand the CISO is to know what they value and what they expect.

Tutorial Objectives

This session helps the storage professional understand the perspective of the security executive. How do they see storage risk? What is their approach to mitigation? We will examine how they challenge conventional wisdom and adapt while assessing threats, assets and vulnerabilities. Then we will look at how they lead in the heat of an incident. Finally, we will provide specific recommendations and offer insight into the best ways for storage professionals to work with the security executive.

After completing this tutorial, you should be able to:

- Better understand information assurance and the CISO “interests” within the storage layer
- Know how security professionals measure storage security and respond to risk and threat
- Understand the upfront and continuing effort required to work with the security team while securing the storage layer

Agenda

- Security Executive Knowledge Base
- What Drives a Security Executive
- Security Executive and the Storage Ecosystem
- Final thoughts

Storage & Security Paradox

SNIA
STORAGE NETWORKING INDUSTRY ASSOCIATION
EDUCATION

Security Executive = Guardian of assets (data)

Storage Professionals = Guardians of Information & Communication Technology (ICT) resources that store and protect data

Although there is a natural synergy …

… positive interaction is not the norm.

The Security Executive

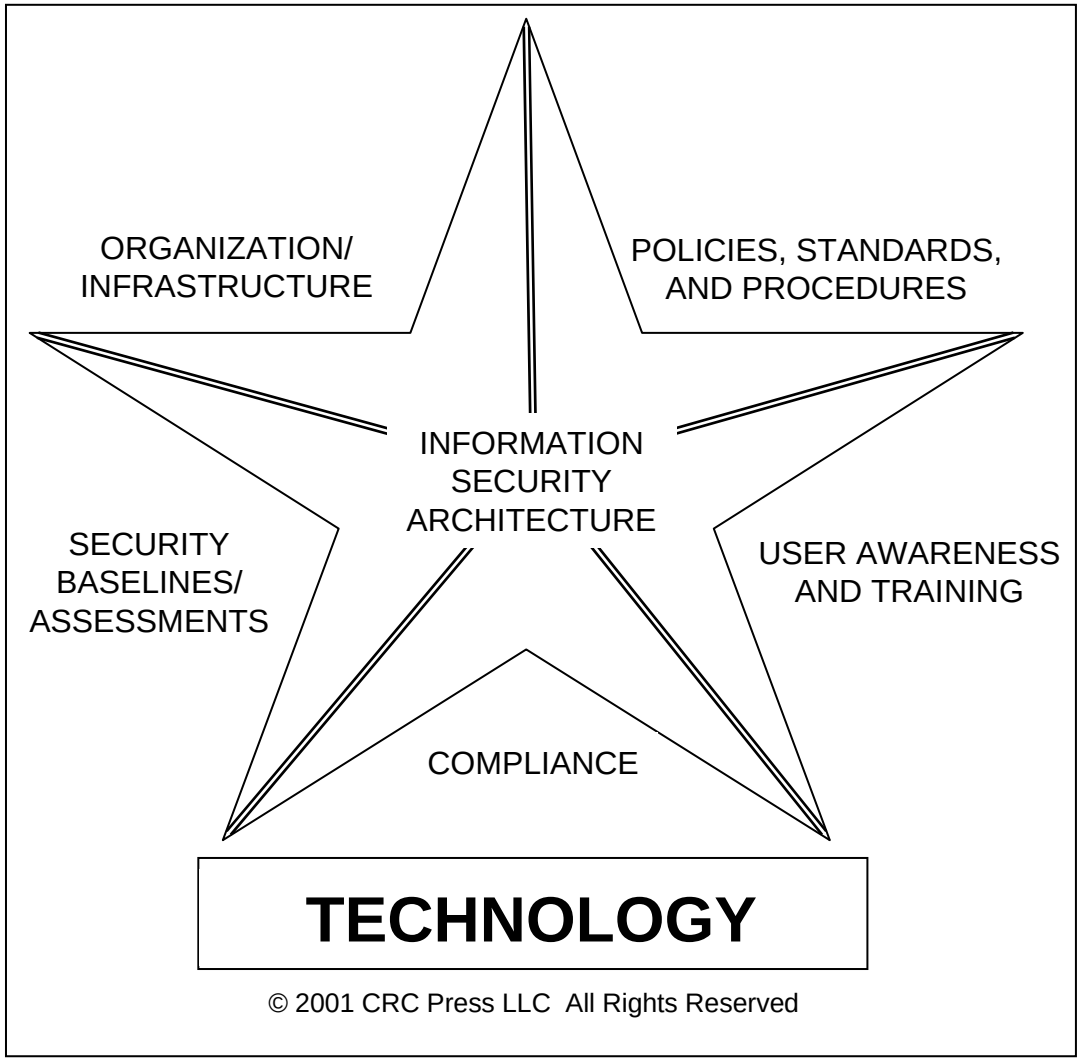
- Chief Security Officer (CSO)
  - A C-level executive, responsible for all aspects of security
  - Typically reports to CEO or possibly COO
  - Involves both physical and information security, including people
  - Focus: Policy, ICT, law, DR/BC, physical protection/safety
  - Background: Often military/former government official
- Chief Information Security Officer (CISO)
  - Senior manager/advisor responsible for traditional Information Security (InfoSec)
  - Often reports to CIO, CTO, or CFO; should be outside of ICT management to be effective
  - Focus: Policy, InfoSec strategy, ICT
  - Background: Often ICT management, InfoSec, ComSec

CSO/CISO Attributes

- The existence of the position signals an elevated importance for security within the organization
- There are no absolutes for the CSO/CISO position
- Many CSO positions are CISO positions
- Less than 50% have budget authority, but almost all have budgetary influence
- Many serve as privacy officers
- About 50% hold one or more security certifications (CISSP, CISM, CISA, GIAC, etc.)

CSO/CISO Knowledge Includes…

Information Security Architecture



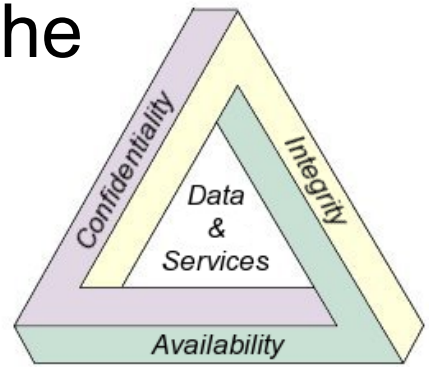
- Five components essential to an effective architecture
- They are the foundation of a secure environment
- They must be fortified with appropriate technology, methods, and programs to ensure that the information is reliable, available, and accessed appropriately on an ongoing basis.

Source: Jan Killmeyer Tudor, *Information Security Architecture – An Integrated Approach to Security in the Organization*, New York. 2001, CRC Press LLC

The Parkerian Hexad

SNIA
Storage Networking Industry Association
EDUCATION

Confidentiality – Privacy of information
Integrity – Correct and/or consistent with the intended state of information
Availability – Timely access to information



Possession – Control over information
Authenticity – Correspondence between data and what the data represent
Utility – Usefulness of data for specific purposes

SOURCE: Donn B. Parker, *Toward a New Framework for Information Security*, The Computer Security Handbook, 4th ed., Seymour Bosworth and M. E. Kabay (New York, 2002)

The Security Paradigm

Principle 1: The Hacker Who Breaks into Your System Will Probably Be Someone You Know

Principle 2: Trust No One, or Be Careful About Whom You Are Required to Trust

Principle 3: Make Would-Be Intruders Believe They Will Be Caught

Principle 4: Protect in Layers

Principle 5: While Planning Your Security Strategy, Presume the Complete Failure of Any Single Security Layer

Principle 6: Make Security a Part of the Initial Design

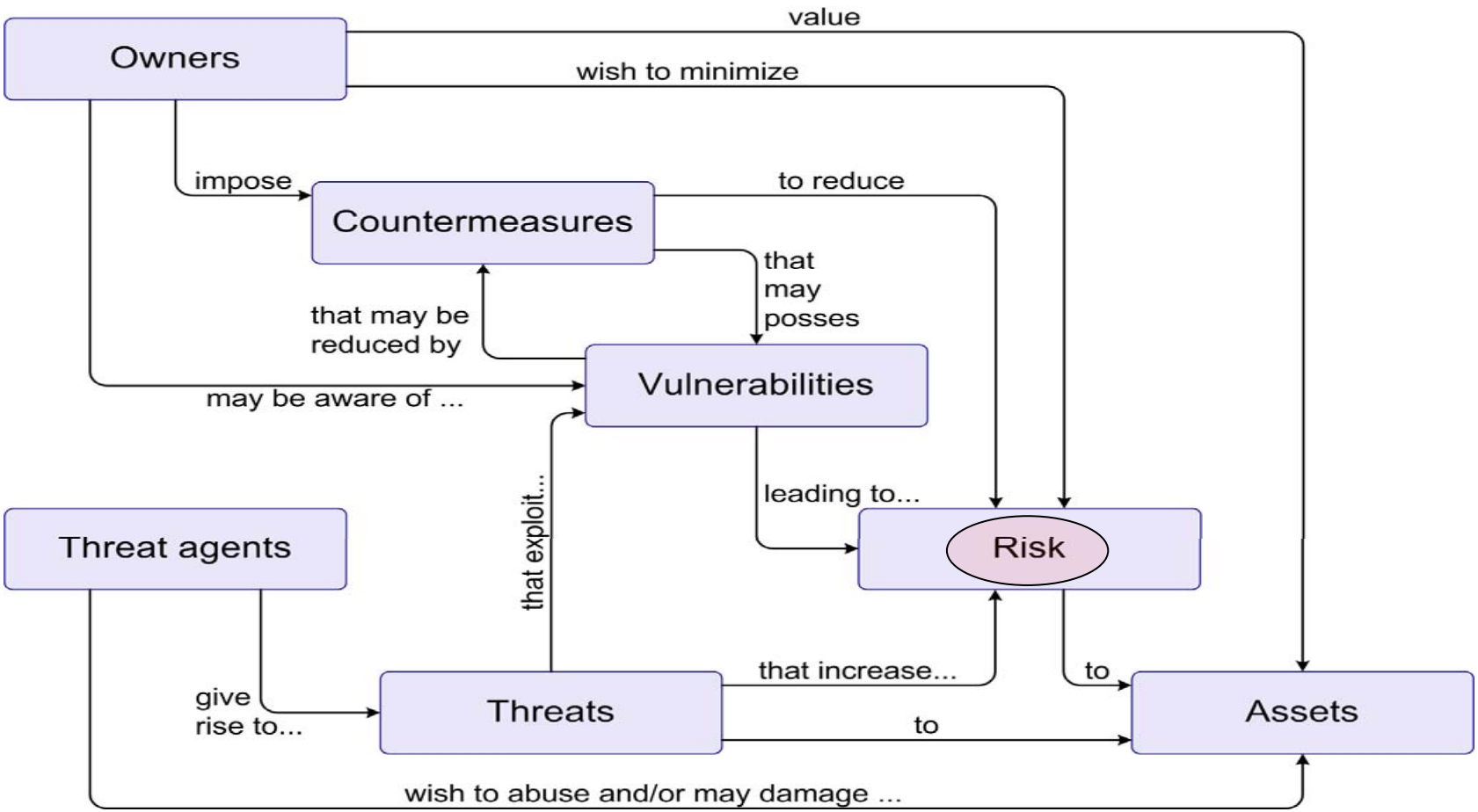
Principle 7: Disable Unneeded Services, Packages, and Features

Principle 8: Before Connecting, Understand and Secure

Principle 9: Prepare for the Worst

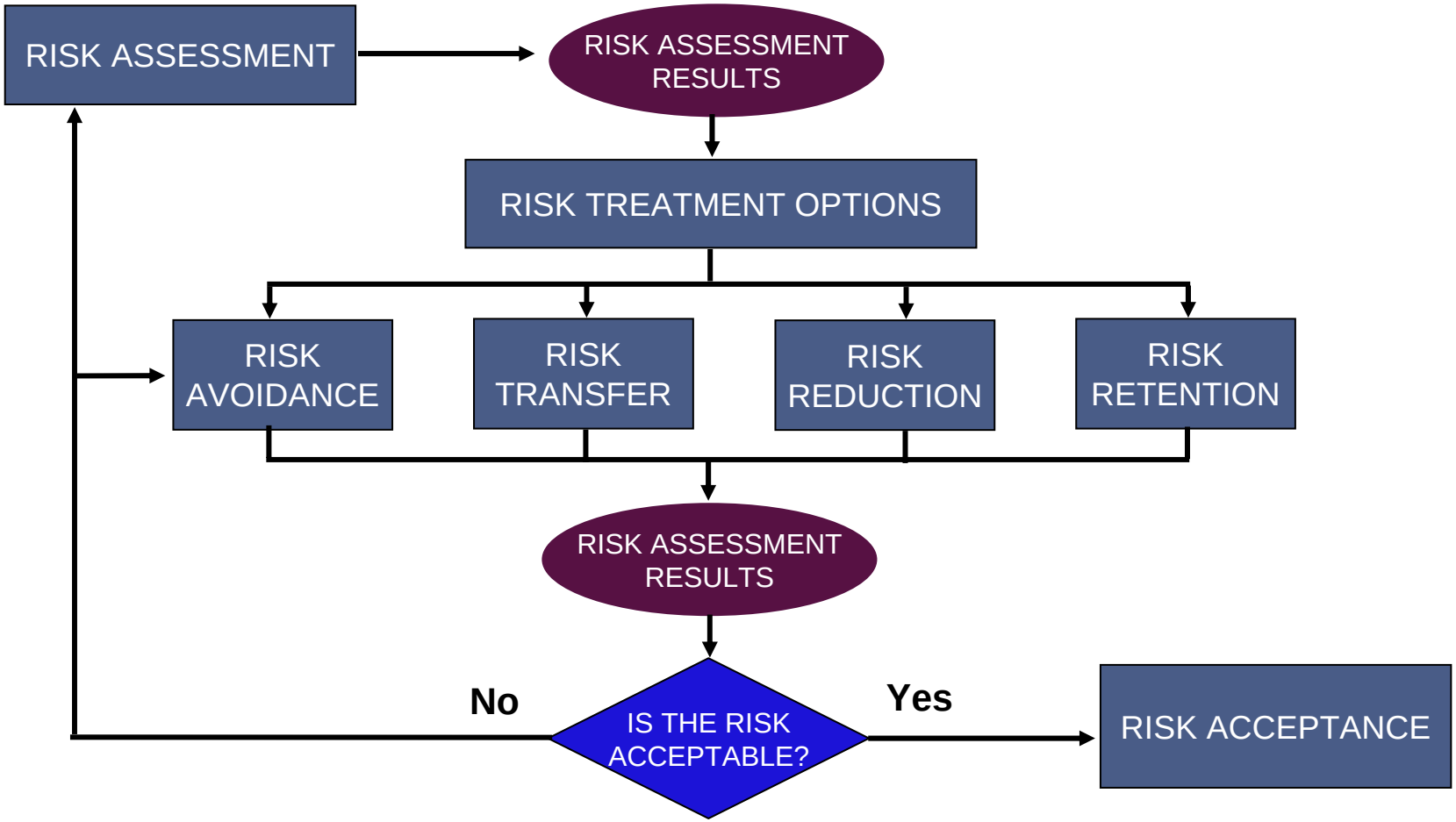
SOURCE: Peter H. Gregory, *Solaris™ Security*," © 2000 by Prentice Hall PTR, ISBN 0-13-096053-5

The Security "Big Picture"



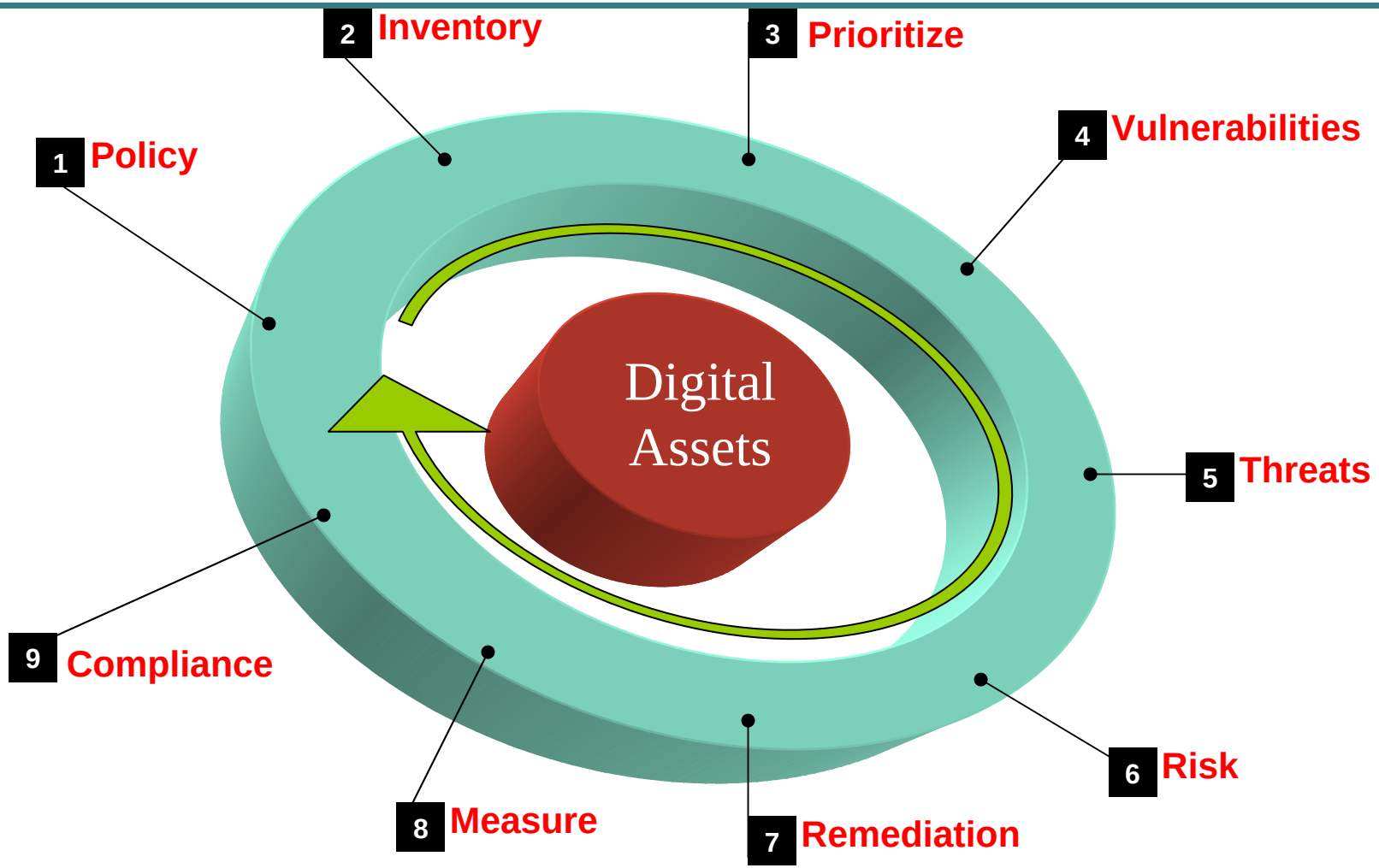
SOURCE: ISO/IEC 15408-1:2005, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model*, Common Criteria v2.3, http://www.iso.ch

Risk Treatment Decision-making Process



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

Risk Management Lifecycle

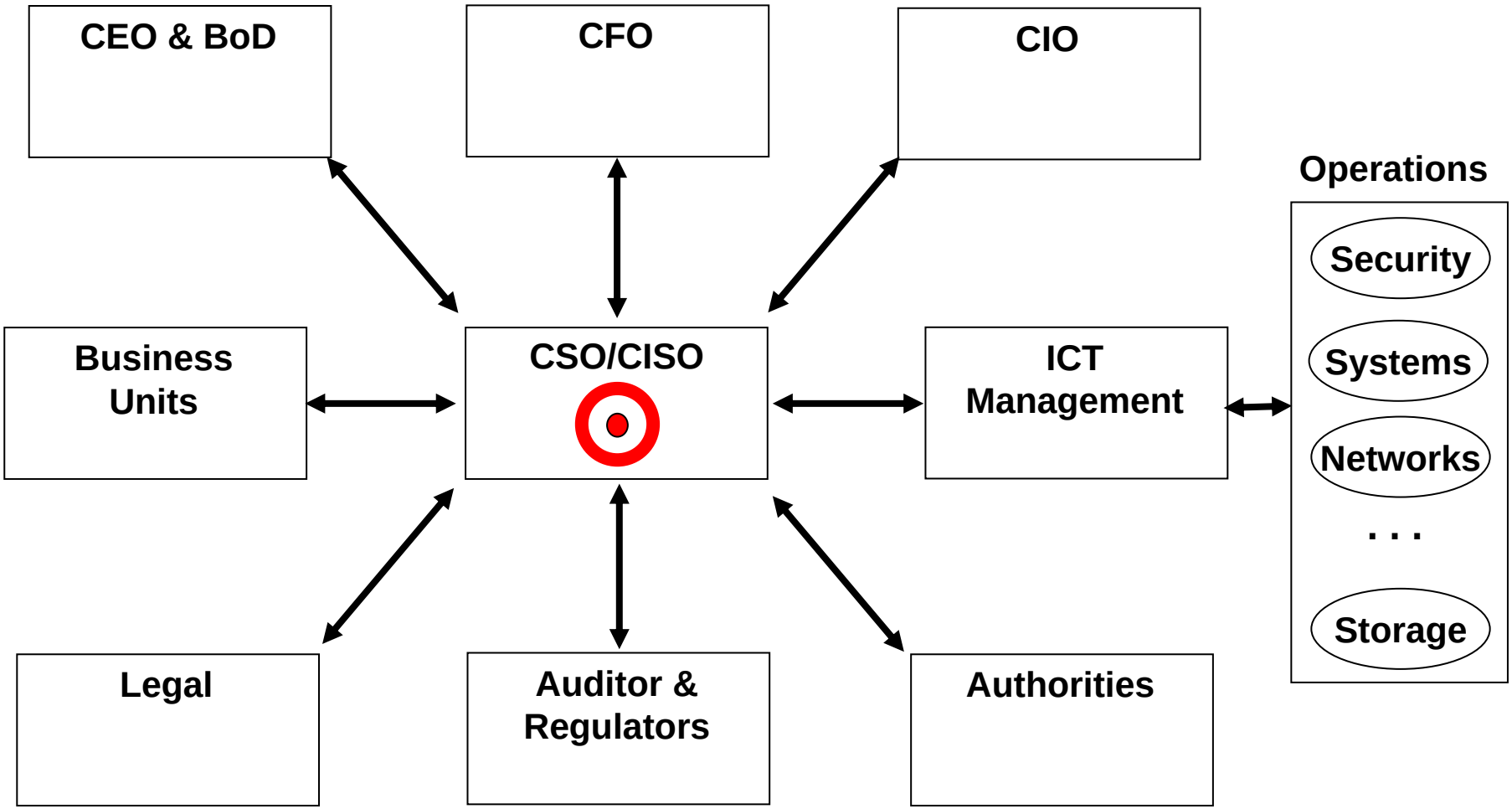


Common Security Frameworks

- ISO/IEC 17799:2005 *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 4.0
- 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

What Drives a CSO/CISO

Dynamic Tension



Security versus 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

Regulatory Drivers
(Sample Domestic US)

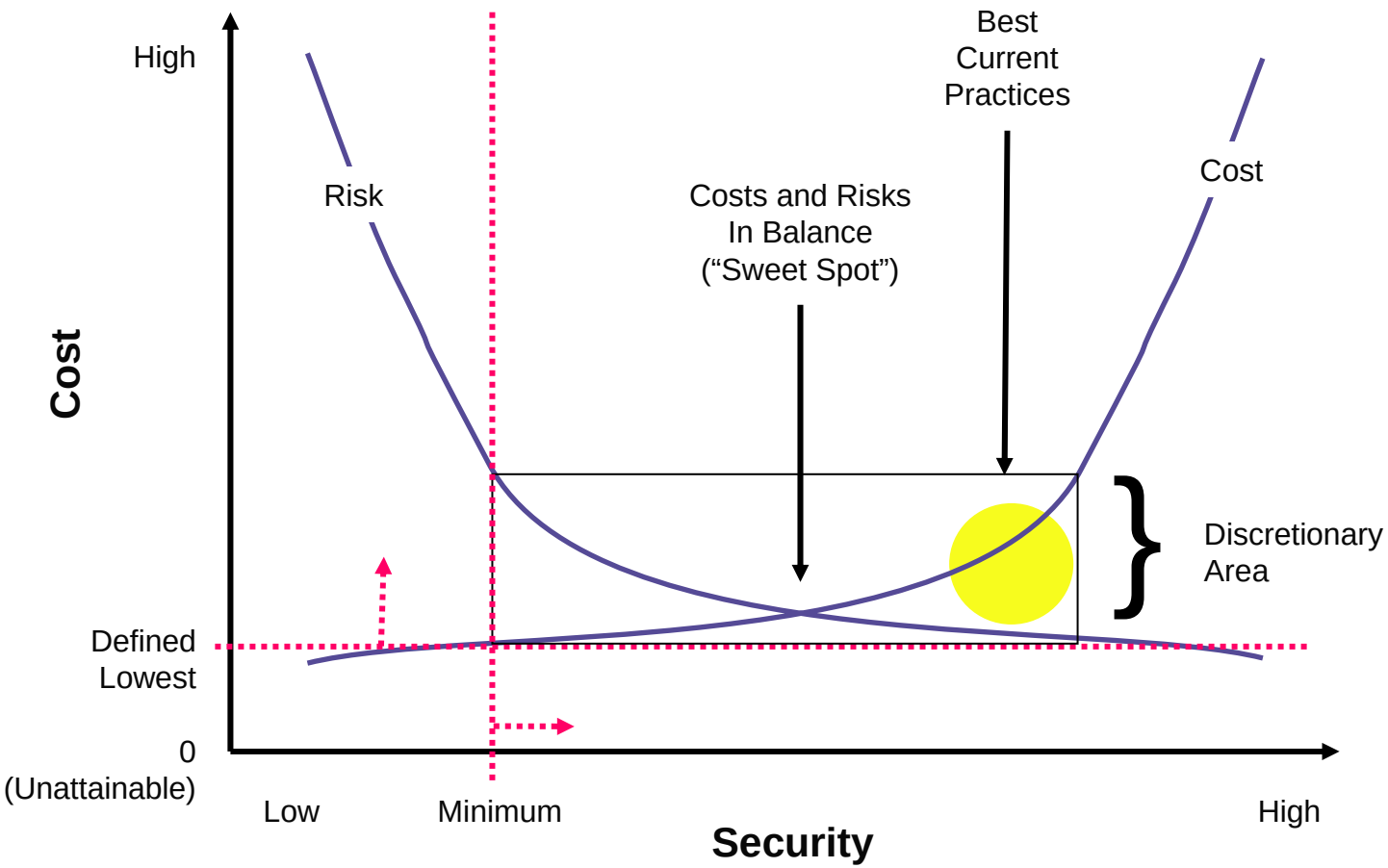
- Sarbanes-Oxley (SOX) Act
- Gramm-Leach-Bliley Act (GLBA)
- Securities Exchange Act (SEC) Rules 17a-3 and 17a-4
- California Data Security Act (SB 1386/AB 1950)
- Health Insurance Portability & Accountability Act (HIPAA)
- DOE 10 CFR 600.153 Retention & Access Requirements for Records
- U.S. Patriot 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

Regulatory Drivers
(Sample International)

SNIA
STORAGE NETWORKING INDUSTRY ASSOCIATION
EDUCATION

- 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

Balancing Cost & Security



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

Standard of Care

- Due Diligence – responsibility one has to investigate and identify issues
  - Are the risks managed appropriately
  - Are the "sensitive" digital assets protected appropriately
  - Are the "critical" digital assets protected appropriately
- Due Care – doing something about the findings from *due diligence*
  - Risk treatment passes the "giggle" test
  - Data protection and data 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

Most Critical Security Issues

(2006 CSI/FBI Top 10)

SNIA
STORAGE NETWORKING INDUSTRY ASSOCIATION
EDUCATION

1. Data protection (e.g., data classification, identification and encryption) and application software (e.g. Web application, VoIP) vulnerability security
2. Policy and regulatory compliance (Sarbanes–Oxley, HIPAA)
3. Identity theft and leakage of private information (e.g. proprietary information, intellectual property and business secrets)
4. Viruses and worms
5. Management involvement, risk management, or supportive resources (human resources, capital budgeting and expenditures)
6. Access control (e.g. passwords)
7. User education, training and awareness
8. Wireless infrastructure security
9. Internal network security (e.g. insider threat)
10. Spyware

SOURCE: Computer Security Institute, *2006 CSI/FBI Computer Crime and Security Survey*," © 2006 by CSI, http://www.gocsi.com

The CSO/CISO and the Storage Ecosystem

Security Meets Storage

SNIA
STORAGE NETWORKING INDUSTRY ASSOCIATION
EDUCATION

- Follow the data and protect appropriately
- Security executives (like many security professionals) know very little about storage ecosystems
- Storage infrastructure and team expected to comply with all ICT security policies and frameworks
- No negative headlines due to security incidents

- Risk … risk … risk … risk …

Risk Exposures
(Potentially Introduced by Storage)

- General Vulnerabilities – Well known security problems; penetration tests used to assess individual systems and applications
- New Attack Vectors – Attackers are moving up the stack, targeting applications (especially Web-based) and specialized elements
- High Value Targets – Aggregation and consolidation of data increases impacts of incidents
- Direct Attacks on Data – Traditional host-based defenses may not be adequate for storage networking

Conformance with Policy

- Applies to all elements of the storage ecosystem
- Sensitivity and criticality of data may invoke additional (more stringent) requirements
- Specific Areas of Interest
  - Least privilege (e.g., role-based access control)
  - Separation of duties (maker-checker)
  - Retention and protection
  - Media sanitization

Compliance

- Storage impacts on compliance activities
  - Failed SOX audit due to inadequate IT controls
  - Implementation of mitigating controls
- Compliance's impact on storage
  - IT acquisitions influenced by feature-set of controls
  - Data retentions increasing storage needs
  - Legacy systems decommissioned

Storage Meets Security

- Limited insight into the data itself
- Many storage professionals have limited security knowledge and infrequent exposures to security
- Solutions for data availability, DR/BC (out-of-region), media sanitization, and data confidentiality
- Data protection efforts produce many copies of the same data (mirrors, replicated copies, backups, VTL, CDP, archive)
- Availability/performance/cost …

From the CSO/CISO

SNIA
STORAGE NETWORKING INDUSTRY ASSOCIATION
EDUCATION

- Policies on data access, protection, retention, sanitization, and management
- Assignment (in writing) of custody of corporate data assets (e.g., owner, authorization, etc.)
- Expected metrics and measurement intervals (i.e., reporting)
- Validation of separation of duties
- Supervision of compensating controls
- Risk evaluation and review (designated security architect)

Final Thoughts

Opportunities for Security & Storage Collaboration

SNIA
STORAGE NETWORKING INDUSTRY ASSOCIATION
EDUCATION

- Storage becomes an important element of the defense-in-depth security strategy
- Storage security measures are effective (not just a checkbox), supportable, and reasonably priced
- Storage contributes to the organization's compliance objectives
- Storage does not become the source of audit surprises (i.e., negative findings)

Last Words

- The weak link in the security chain is most often the human element. Security IS a people problem!
- Manage the risks or mitigate the consequences
- A holistic approach to security includes the people, the organization, governance, process and, lastly, technology.
- Expectations of the security program - keeping the organization out of trouble and out of the headlines, while doing it for as little money possible
- Implementing firewalls and hardening systems are not really security issues any longer but operational issues

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
Richard Austin, CISSP
LeRoy Budnik, CISA
Phil Huml

SNIA Security TWG

Andrew Nielsen, CISSP
Larry Hofer, CISSP
Roger Cummings

SNIA SSIF

SNIA Security

SNIA
STORAGE NETWORKING INDUSTRY ASSOCIATION
EDUCATION

- 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

Security Framework Sources

- ISO/IEC 27000 Series (www.iso.org) – Information security management systems
- COBIT® v4.0 (www.isaca.org/cobit) – Control Objectives for Information and related Technology
- COSO (www.coso.org) – Enterprise Risk Management — Integrated Framework
- FFIEC (www.ffiec.gov) – FFIEC Information Technology Examination Handbook
- NIST/CSD Computer Security Resource Center (csrc.nist.gov/publications/nistpubs) – Security standards for U.S. Government
- CICA (www.cica.ca) – Information Technology Control Guidelines (ITCG)
- ITIL (www.itil.co.uk) – ITIL Security Management

Additional Sources of Security Information

SNIA
STORAGE NETWORKING INDUSTRY ASSOCIATION
EDUCATION

- 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 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

