Education

Introduction to Information Assurance

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 Information Assurance

- Many organizations face the task of implementing data protection and data security measures to meet a wide range of requirements. With increasing frequency, storage managers and professionals are being asked to handle elements of this protection, which are often presented in the form of a security checklist. However, checklist compliance by individuals who are missing a basic background in Information Assurance is a quick recipe for trouble.
- At its core, Information Assurance is about ensuring that authorized users have access to authorized information at the authorized time. Further, it doesn't matter whether the information is in storage, processing, or transit, and whether threatened by malice or accident. This session provides an introduction to Information Assurance as well as details that will help storage personnel better understand its applicability in their own environments.

A Little Background…

- Previously, SNIA included an *Introduction to Storage Security* tutorial, which focused on basic concepts and best practices
- The focus has now shifted to foster improved interactions with the security and audit professionals
- Storage security best practices are presented in a separate tutorial that mirrors the SNIA Technical Proposal on the subject

What is Information Assurance (IA)?

- Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation.
- These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

SOURCE: National Information Assurance Glossary (CNSS Instruction No. 4009)

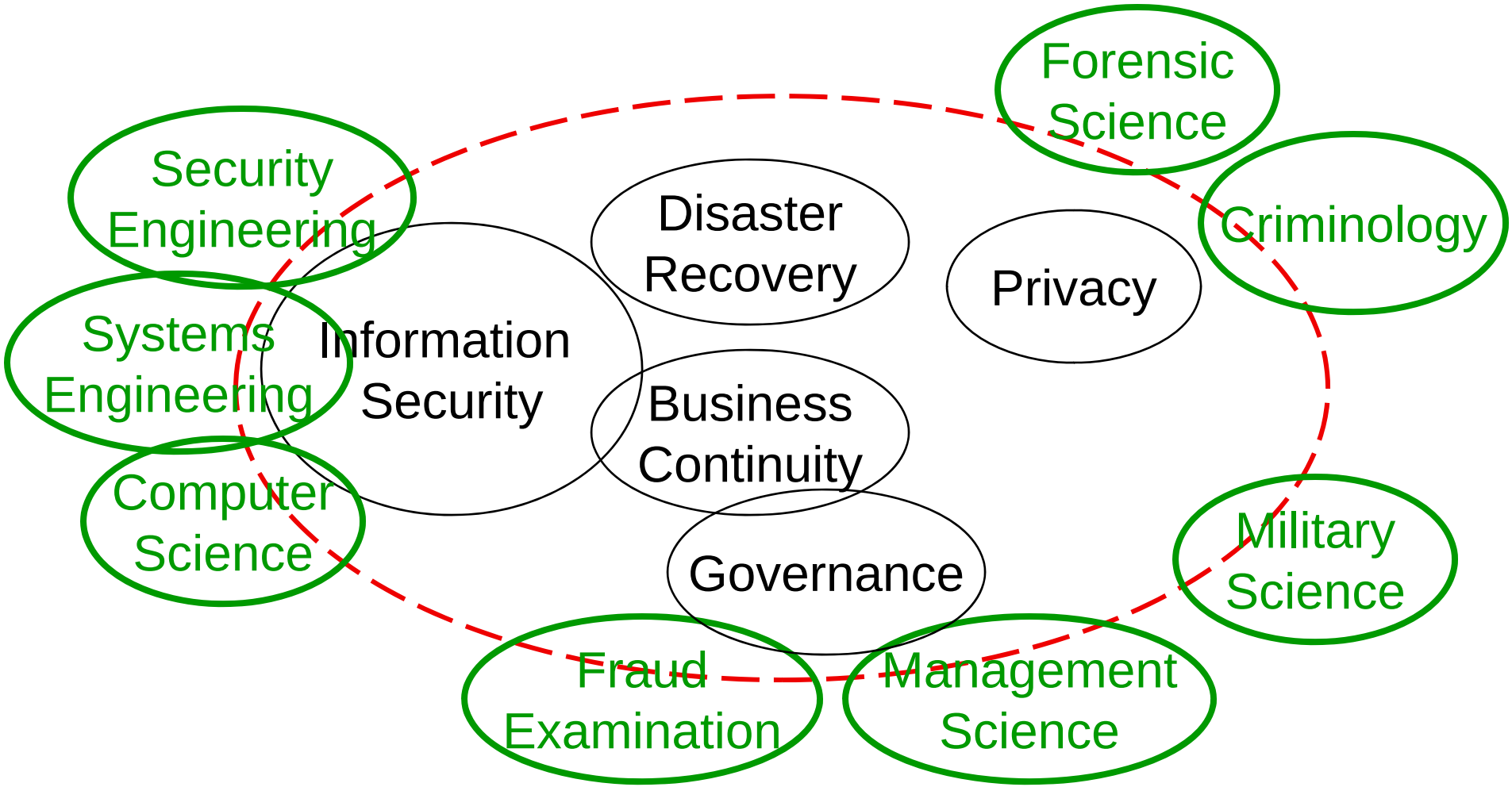
What is Information Assurance (IA)?

Education SNIA

- Information assurance defines and applies a collection of policies, standards, methodologies, services, and mechanisms to maintain mission integrity with respect to people, process, technology, information, and supporting infrastructure.
- Information assurance provides for confidentiality, integrity, availability, possession, utility, authenticity, nonrepudiation, authorized use, and privacy of information in all forms and during all exchanges.

Source: Information Assurance Architecture, Keith D. Willett, 2008, CRC Press, ISBN: 978-0-8493-8067-9

Aspects of Information Assurance



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

IA Architecture (IA^2) Framework

- Basic conceptual structure for defining and describing an information assurance architecture
- Risk (root driver) may be expressed in terms of business drivers and technical drivers
- Six architectural views: people, policy, business process, system and application, information/data, and infrastructure

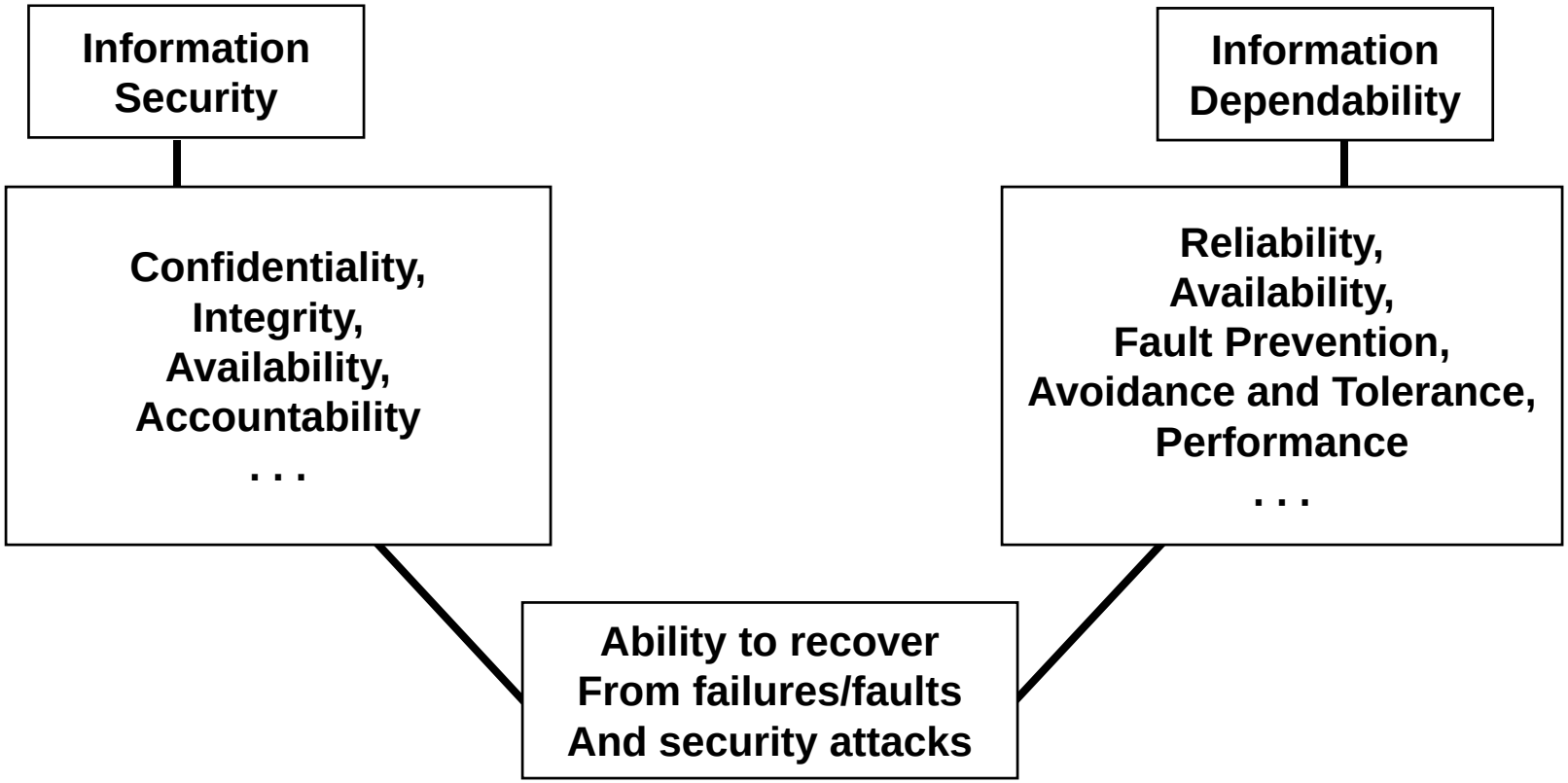
- A single statement of risk may be stated from the perspective of nine IA Core Principles, each from one of the six different IA^2 views, or 54 perspectives on that single risk.

Information Assurance Process

- Enumeration and classification of the information assets (e.g., data/information technology and value)
- Risk assessment (vulnerabilities and threats)
- Risk analysis (probabilities/likelihood and impacts)
- Risk management (treatment)
- Test and review

- Repeat…

Information Assurance



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

A Few Words on Information Security

IA vs. Information Security (InfoSec)

- Both involve people, processes, techniques, and technology (i.e., administrative, technical, and physical controls)
- Information assurance and information security are often used interchangeably (incorrectly)
- InfoSec is focused on the confidentiality, integrity, and availability of information (electronic and non-electronic)
- IA has broader connotations and explicitly includes reliability, access control, and nonrepudiation as well as a strong emphasis on strategic risk management

- ISO information security management standards (ISMS) are more closely aligned with IA

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

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

Basic Security Concepts & Principles

- 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

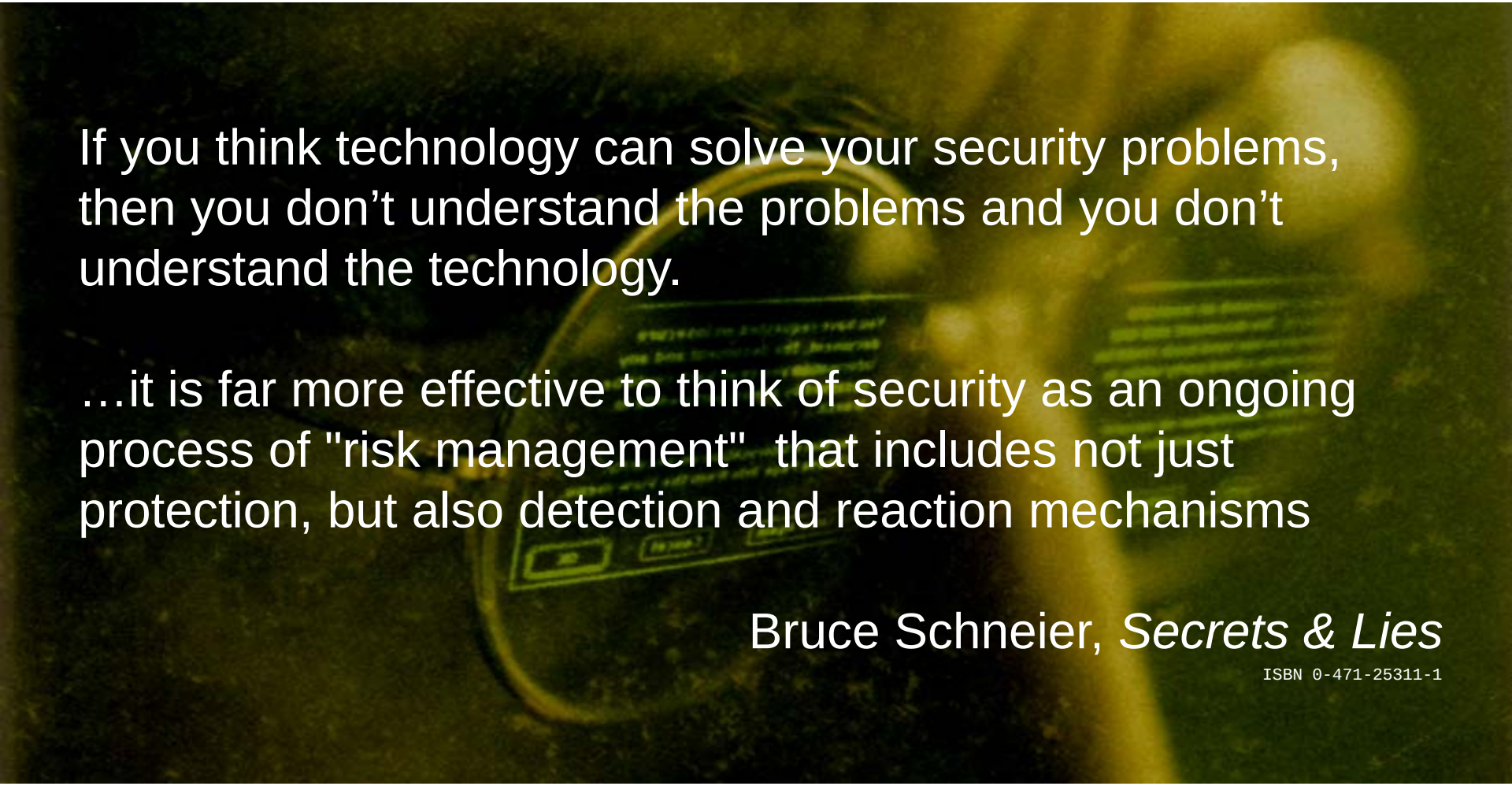
Basic Security Concepts & Principles

- 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

Approaches to Applying Principles

- *Security by Obscurity Strategy*
  - Basic premise is stealth / hiding
- *The Perimeter Defense Strategy*
  - More of a concentrated effort in defense
  - Defense between "insiders" and "outsiders"
- *Defense in Depth Strategy* (Recommended)
  - Employs a number of operationally interoperable and complementary technical and non-technical layers of defense
  - May use enclaves for stronger regions of defense

Security is People-based Problem



If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

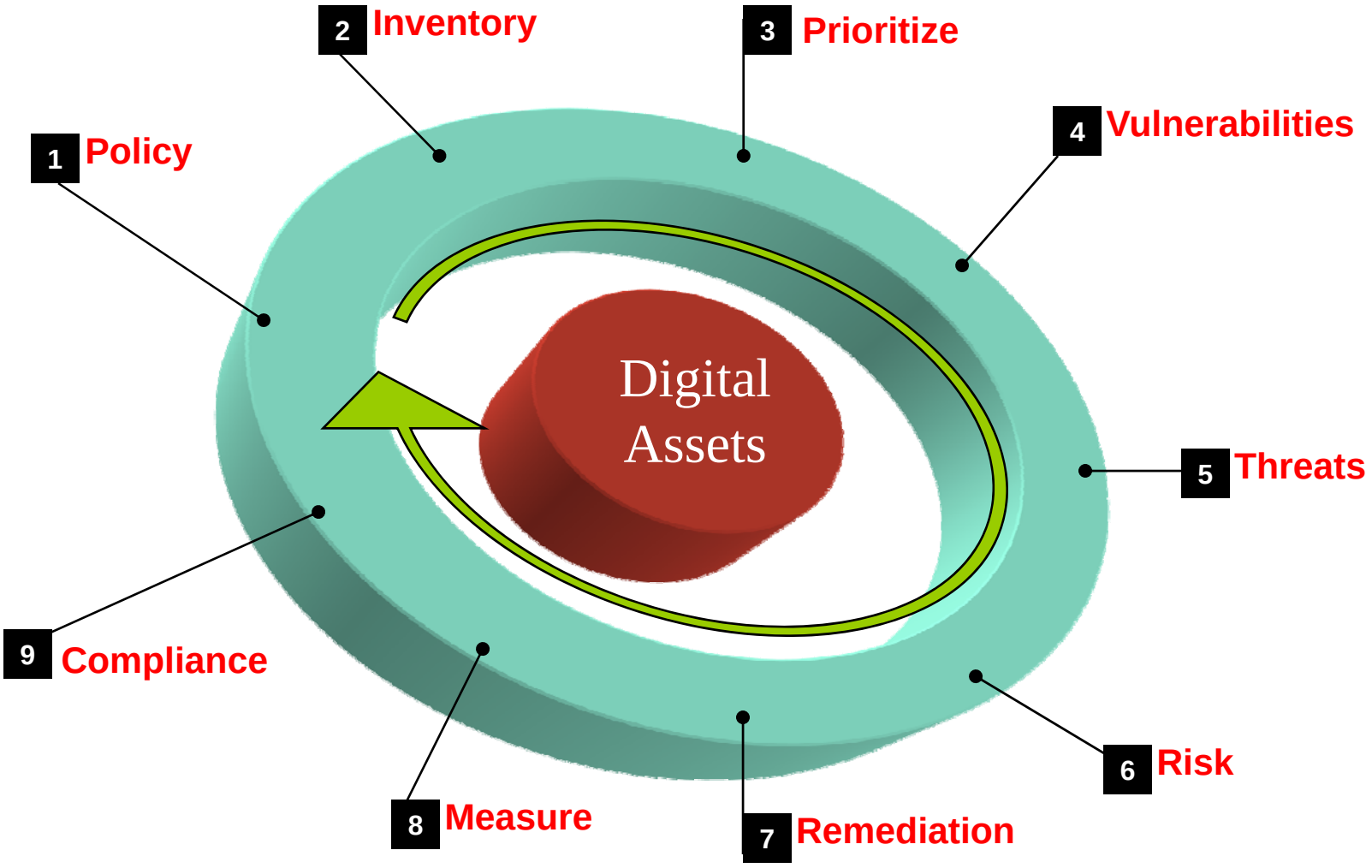
…it is far more effective to think of security as an ongoing process of "risk management" that includes not just protection, but also detection and reaction mechanisms

Bruce Schneier, *Secrets & Lies*

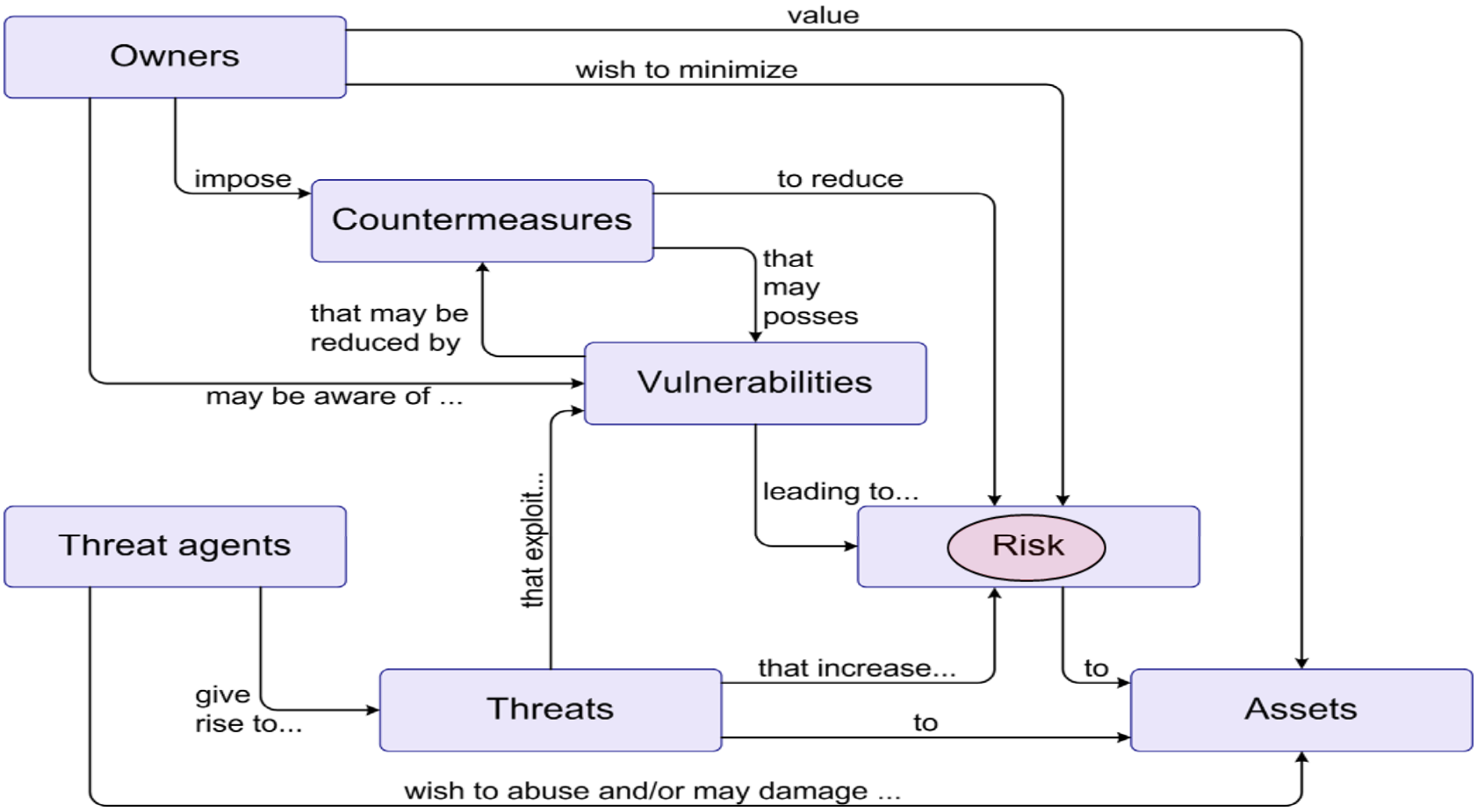
ISBN 0-471-25311-1

A Few Words on Risk

Risk Management Lifecycle

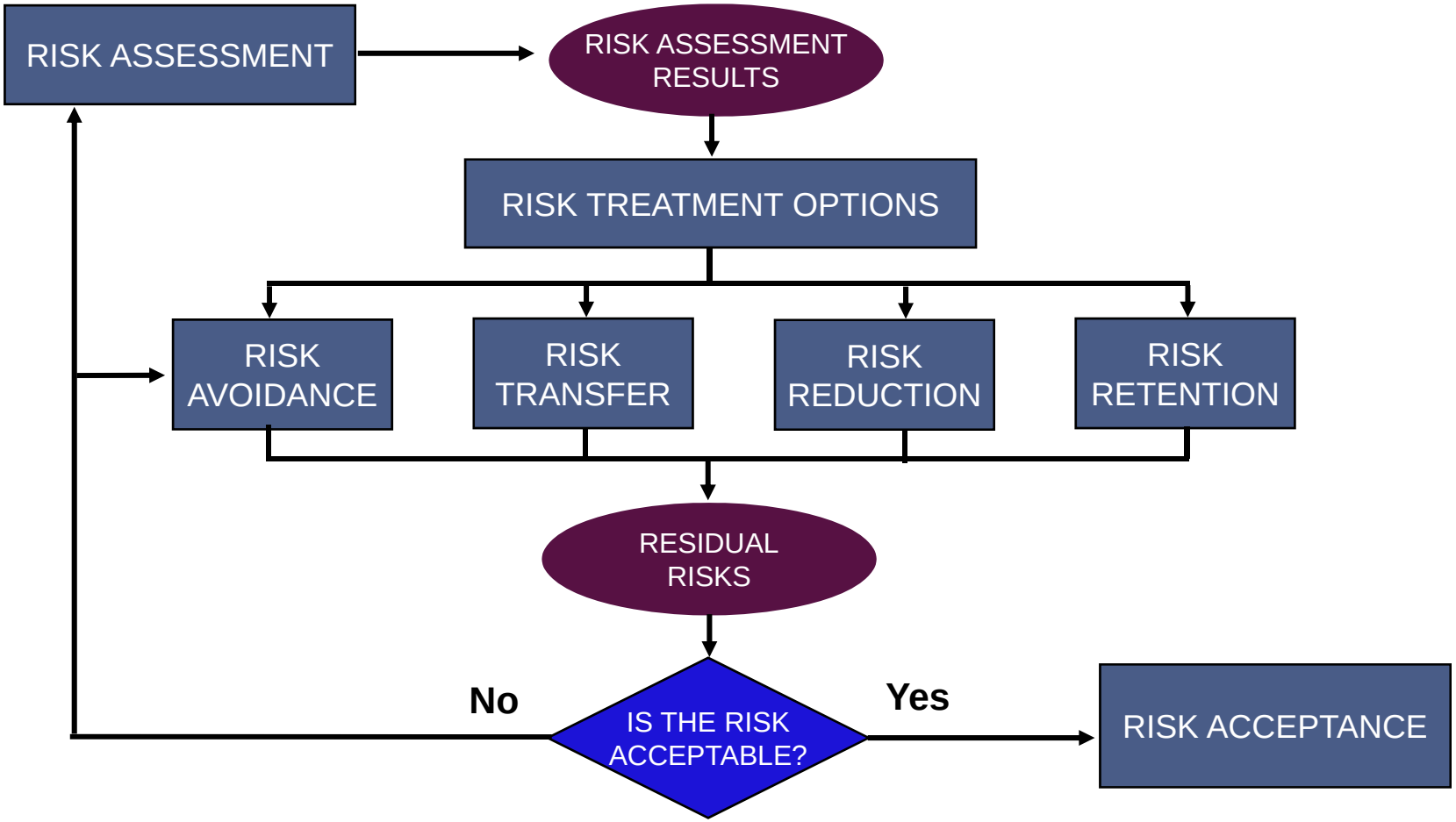


The Security "Big Picture"



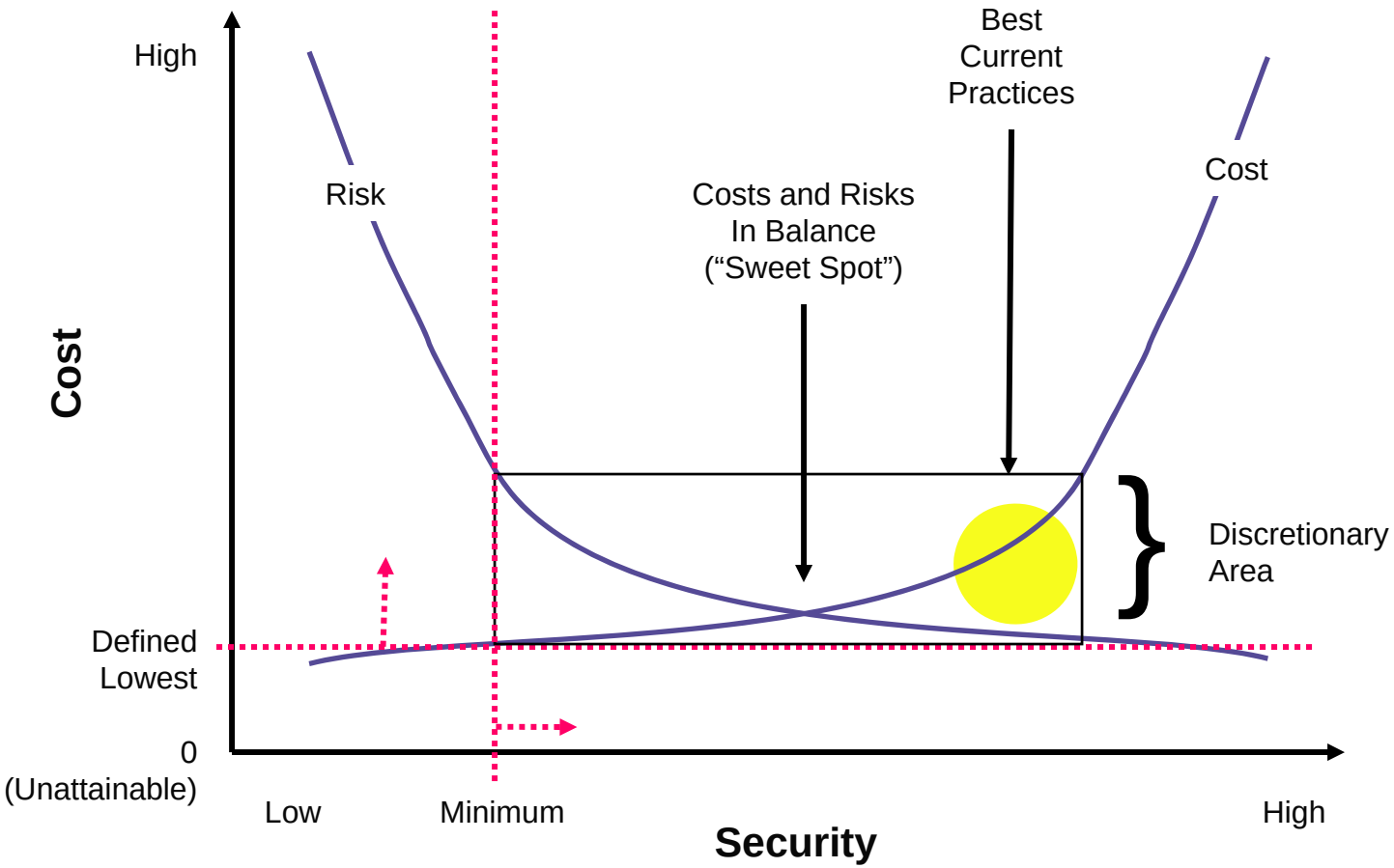
SOURCE: ISO/IEC 15408-1:2005, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model*, Common Criteria v2.3, http://www.iso.ch

Risk Treatment Decision-making Process



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

Balancing Cost & Risk



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

Final Thoughts

Information Assurance Summary

- The root driver behind IA is risk
- Effective IA requires integration from inception and not after-the-fact *bolt-ons*
- Good business practice is the complement to compliance requirements

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

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

Ray Kaplan, CISSP

For More Information

SNIA Security

- 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

Useful Printed Resources

- *Information Assurance Architecture*, Keith D. Willett, 2008, CRC Press, ISBN: 978-0-8493-8067-9
- *Information Assurance – Managing Organizational IT Security Risks*, Joseph G. Boyce and Dan W. Jennings, 2002, Butterworth Heinemann, ISBN: 0-7506-7327-3
- *Information Assurance – Dependability and Security in Networked Systems*, Qian, Joshi, Tipper, Krishnamurthy, 2008, Morgan Kaufmann, ISBN: 978-0-12-373566-9
- *A Practical Guide to Security Engineering and Information Assurance*, Debra S. Herrmann, 2001, Auerbach Publications, ISBN: 978-0-8493-1163-5
- *Information Security Architecture – An Integrated Approach to Security in the Organization*, Jan Killmeyer Tudor, 2001, AUERBACH, ISBN: 978-0-8493-9988-6
- *Enterprise Security Architecture – A Business-Driven Approach*, Sherwood, Clark, Lynas, 2005, CPM Books , ISBN: 978-1-57820-318-5