Overview

- The CIA
- Security Governance
  - Policies, Procedures, etc.
  - Organizational Structures
  - Roles and Responsibilities
- Information Classification
- Risk Management
The CIA: Information Security Principles

- Confidentiality
  - Allowing only authorized subjects access to information

- Integrity
  - Allowing only authorized subjects to modify information

- Availability
  - Ensuring that information and resources are accessible when needed
Confidentiality
- Preventing unauthorized subjects from accessing information

Integrity
- Preventing unauthorized subjects from modifying information

Availability
- Preventing information and resources from being inaccessible when needed
Think in terms of the core information security principles

How does this threat impact the CIA?

What controls can be used to reduce the risk to CIA?

If we increase confidentiality, will we decrease availability?
Security Governance is the organizational processes and relationships for managing risk

- Policies, Procedures, Standards, Guidelines, Baselines
- Organizational Structures
- Roles and Responsibilities
Laws, Regulations, Requirements, Organizational Goals, Objectives

General Organizational Policies

Functional Policies

Procedures  Standards  Guidelines  Baselines
Policies are statements of management intentions and goals

- Senior Management support and approval is vital to success
- General, high-level objectives
- Acceptable use, internet access, logging, information security, etc
Procedures

- Procedures are detailed steps to perform a specific task.
- Usually required by policy.
- Decommissioning resources, adding user accounts, deleting user accounts, change management, etc.
Standards specify the use of specific technologies in a uniform manner.

Requires uniformity throughout the organization.

Operating systems, applications, server tools, router configurations, etc.
Guidelines

- Guidelines are recommended methods for performing a task
- Recommended, but not required
- Malware cleanup, spyware removal, data conversion, sanitization, etc
Baselines are similar to standards but account for differences in technologies and versions from different vendors.

Operating system security baselines

- FreeBSD 6.2, Mac OS X Panther, Solaris 10, Red Hat Enterprise Linux 5, Windows 2000, Windows XP, Windows Vista, etc.
Organizational Structure

- Organization of and official responsibilities for security vary
  - BoD, CEO, BoD Committee
  - CFO, CIO, CSO, CISO
  - Director, Manager

- IT/IS Security

- Audit
Board of Directors/Trustees -> President

CIO

Security Director

Project Security Architect
Enterprise Security Architect
Security Analyst
System Auditor
Organizational Structure

- Audit should be separate from implementation and operations
  - Independence is not compromised
- Responsibilities for security should be defined in job descriptions
- Senior management has ultimate responsibility for security
- Security officers/managers have functional responsibility
Roles and Responsibilities

- Best Practices:
  - Least Privilege
  - Mandatory Vacations
  - Job Rotation
  - Separation of Duties
Roles and Responsibilities

- **Owners**
  - Determine security requirements

- **Custodians**
  - Manage security based on requirements

- **Users**
  - Access as allowed by security requirements
Information Classification

- Not all information has the same value
- Need to evaluate value based on CIA
- Value determines protection level
- Protection levels determine procedures
- Labeling informs users on handling
Government classifications:

- Top Secret
- Secret
- Confidential
- Sensitive but Unclassified
- Unclassified
Private Sector classifications:

- Confidential
- Private
- Sensitive
- Public
Information Classification

Criteria:

- Value
- Age
- Useful Life
- Personal Association
Risk Management is identifying, evaluating, and mitigating risk to an organization

- It’s a cyclical, continuous process
- Need to know what you have
- Need to know what threats are likely
- Need to know how and how well it is protected
- Need to know where the gaps are
Assets

Threats
  • Threat-sources: man-made, natural

Vulnerabilities
  • Weakness

Controls
  • Safeguard
Quantitative

- Objective numeric values
- Cost-Benefit analysis
- Guesswork low

Qualitative

- Subjective intangible values
- Time involved low
- Guesswork high
Remedy/Mitigation

- Reduce
  - Use controls to limit or reduce threat

- Remove
  - Stop using it

- Transfer
  - Get insurance or outsource it

- Accept
  - Hope for the best
Security Management practices involve balancing security processes and proper management and oversight.

Risk Management is a big part of managing holistic security of an organization.