Risk Management

Chapter 4

Risk Management

- Risk identification
  - "The process of examining & documenting the security posture of an organization's information technology and the risks it faces."
- Risk assessment
  - "determination of the extent to which the organization's information assets are exposed or at risk."
- Risk control
  - "application of controls to reduce the risks to an organization's data and information systems.

Risk Management

Risk Identification

- Identify and Inventory Assets
- Classify and prioritize assets
- Identify and prioritize threats

Risk Assessment

- Identify vulnerabilities between assets and threats
- Identify and quantify asset exposure

Risk Control

- Select strategy
- Justify Controls
- Implement and monitor controls

Communities of Interest

- community of people who share a common interest or passion [Wikipedia]
- Community of Interest for Information Security
  - Management and users
- Responsibilities
  - Early detection and response
  - Provide sufficient resources (management)
  - Identify most important resources from a user perspective
  - Build secure systems
  - Operate secure systems
  - Evaluating the risk controls
  - Determine which control options are cost effective
  - Acquiring or installing the needed controls
  - Ensuring the controls remain effective
  - Conduct periodic management reviews
  -

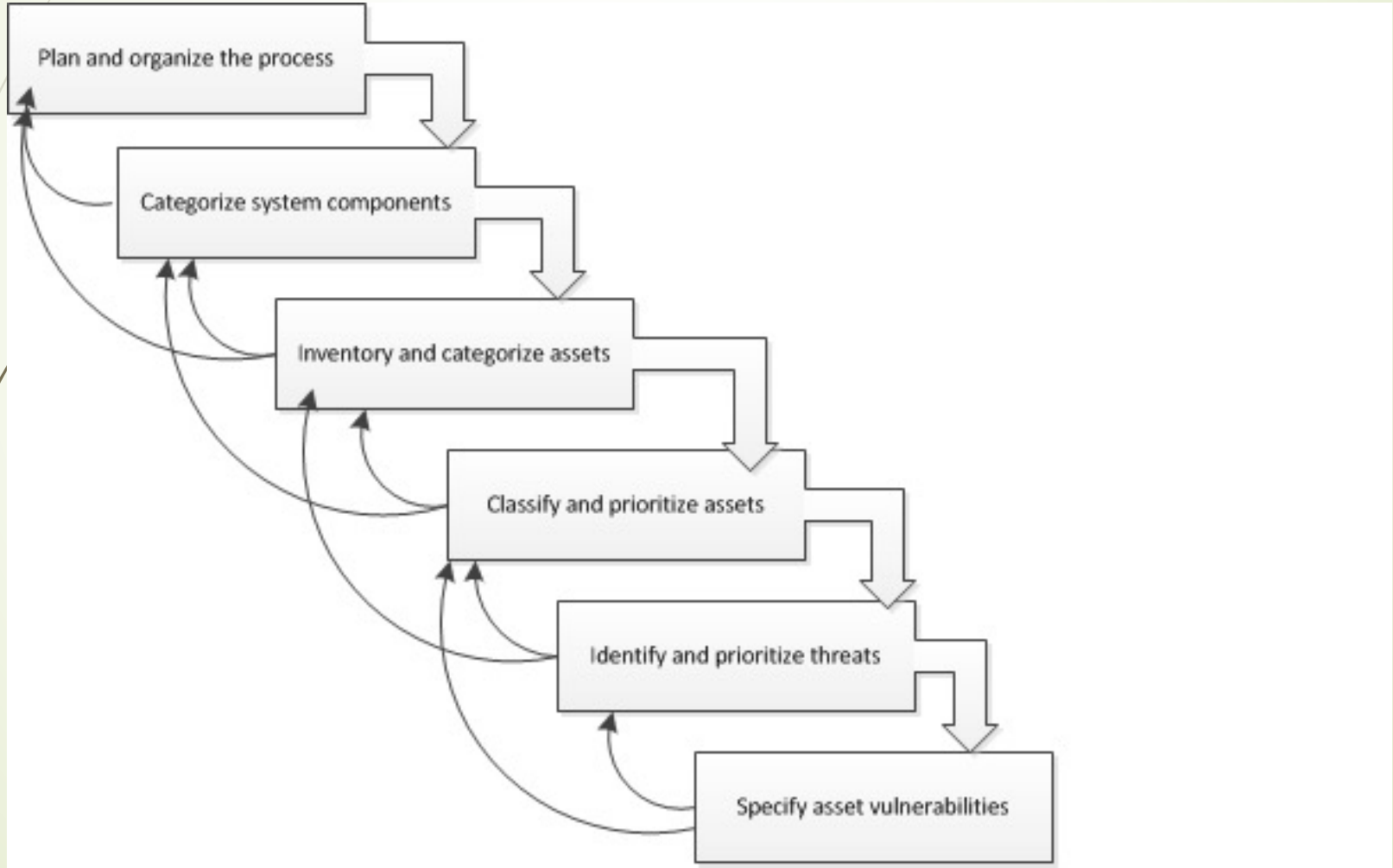
Competitiveness

- Information Technology Role
  - Began as a advantage
  - Now falling behind is a disadvantage
- Availability is a necessity

Risk Management

- Know yourself
  - Understand the technology and systems in your organization
- Know the enemy
  - Identify, examine, understand threats
- Role of Communities of Interest
  - Information Security
  - Management and Users
  - Information Technology

Risk Identification Components



Asset Identification & Valuation

People	Employee	Trusted employees Other staff
	Non-employees	People at trusted organizations / Strangers
Procedures	Procedures	IT & business standards procedures IT & business standards procedures
Data	Information	Transmission, Processing, Storage
Software	Software	Applications, Operating systems, Security components
Hardware	System devices and peripherals	Systems and peripherals Security devices
	Networking components	Intranet components Internet or DMZ components

Asset Identification

- People: Position name/number ID
  - Try to avoid names
- Procedures
  - Intended purpose
  - Relationship to software, hardware, network elements
  - Storage location
- Data
  - Owner, creator, manager, size, structure location, backup procedure, on-off line

Hardware, Software, Network Asset Id

- Name (device or program name)
- IP address
- Media access control (MAC) address
- Element type – server, desktop, etc
  - Device Class, Device OS, Device Capacity
- Serial number
- Manufacturer name
- Manufacturer model or part number

Hardware, Software, Network Asset Id

- Software version, update revision
- Physical location
- Logical location
  - Where on network
- Controlling entity
  - Organization unit to which it belongs

Information Asset Classification

- Classification must be specific enough to allow determination of priority
- Comprehensive – all info fits in list somewhere
- Mutually exclusive – fits in one place

Determination of Value

- Cost of creating the information asset
- Retained from past maintenance of information asset
- Implied by the cost of replacing information
- Value from providing the information
- Value to owners
- Intellectual property value
- Value to adversaries

Ordering by Importance

- Weighted factor analysis
- Each info asset assigned score for each critical factor (0.1 to 1.0)
  - Impact to revenue
  - Impact to profitability
  - Impact to public image
- Each critical factor is assigned a weight (1-100)
- Multiple and add
- Table 4.2 – page 122

Data Classification & Management

- Determine a classification scheme
  - Confidential
  - Internal
  - External
- Assign classification to all data
- Grant access to data based on classification and need
- Devise some method of managing data relative to classification

Threat and Prioritize Threats & Threat Agents

Threat	Examples
Compromises to intellectual property	Piracy, copyright infringement
Espionage or trespass	Unauthorized access
Forces of nature	Fire, flood, earthquake, lightning
Human error or failure	Accidents, mistakes, etc
Missing, inadequate, incomplete controls	Training, privacy, ineffective policy
Deviation of quality of service	Power and WAN quality of service
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, DOS
Technical hardware failures	Equipment failures
Technical software failures	Bugs, code problems, loopholes
Technological obsolescence	Antiquated or outdated technology
Theft	Illegal confiscation of property

Threat Assessment

- Each treat must be examined to asses potential damage
  - Which threats present a danger to an organization's assets?
  - Which threats represent the most danger - probability of attack?
  - How much would it cost to recover?
  - Which treat requires the greatest expenditure to prevent?

Vulnerability Identification

- Id each asset and each threat it faces
- Create a list of vulnerabilities
- Examine how each of the threats are likely to be perpetrated

Risk Assessment

Risk =

likelihood of occurrence of vulnerability

*

value of the information asset

-

% of risk mitigated by current controls

+

uncertainty of current knowledge of vulnerability.

Likelihood

- Probability that a specific vulnerability within an organization will be successfully attacked
- Assign number between 0.1 – 1
- Data is available for some factors
  - Likelihood of fire
  - Likelihood of receiving infected email
  - Number of network attacks

Valuation of Information Assets

- Using info from asset identification assign weighted score for the value
  - 1 -100
  - 100 – stop company operations
  - May use broad categories
  - NIST has some predefined

Problem

Information asset A has a value score of 50 and has one vulnerability. Vulnerability 1 has a likelihood of 1.0 with no current controls. You estimate the assumptions and data are 90% accurate

Solution – Problem 1

Asset A = (50 X 1.0)–0% + 10%

= (50 X 1.0)– ((50 X 1.0)X0) +((50 X 1.0)+.1)

= 50 – 0 + 5

= 55

Problem

- Information asset B has a value score of 100 and has two vulnerability.
  - Vulnerability 2 has a likelihood of 0.5 with current controls address 50% of its risk,
  - Vulnerability 3 has a likelihood of 0.1 with no current controls, & you estimate the assumptions and data are 80% accurate

Solutions

Asset B (V2) = (100 X .5)– 50% + 20%

= (100 X .5)-((100 X0.5) X 0.5) + ((100 X 0.5) X 0.2)

= 50 – 25 +10

= 35

Asset B (V3) = (100 X .1)– 0% + 20%

= (100 X .1)-((100 X0.1) X 0) + ((100 X 0.1) X 0.2)

= 12

Identify Possible Controls

- Residual risk – risk remaining after controls are applied
- 3 categories of controls
  - Policies
  - Programs
  - Technologies
- Policies – documents that specify an organization's approach to security
- Programs – activities performed within the organization to improve security
- Technologies – technical implementations of the policies
- Access control – fundamental to IS process
  - Considered a simple function of the system

Documenting Results of Risk Assessment

- Summarized document
- Rank vulnerability worksheet
- Contents
  - Asset – list each vulnerable asset
  - Asset impact
  - Vulnerability: list uncontrolled vulnerabilities
  - Vulnerability likelihood
  - Risk-rating factor (asset impact * likelihood)
- Order by risk-rating factor

Risk Control Strategies

- 5 basic strategies
  - Defend: attempt to prevent the exploitation of the vulnerability
  - 3 common methods
    - Application of policy
    - Education and training
    - Application of technology
  - Transfer: shift the risk to other areas or outside entities
  - Mitigate: Reduce the impact should the vulnerability be exploited
    - Planning and preparation
    - Early detection
    - Quick, efficient, and effective response
  - Accept: Choose to do nothing
  - Terminate: avoid those business activities that introduce uncontrollable risk

Selecting a Risk Control Strategy

- Feasibility Studies
  - Explore the consequences
- Cost Benefit Analysis (CBA)
- Benchmarking and Best Practices
- Baselining

Feasibility Studies

- Compare cost to potential loss
- Cost avoidance is the process of avoiding the financial impact of an incident

Cost Benefit Analysis

- Evaluate worth of asset
- Loss of value if asset compromised
- Items affecting cost of control
  - Cost of development or acquisition
  - Cost of implementation
  - Services costs
  - Cost of maintenance
- Benefits – value gained by using controls

Cost Benefit Analysis

- Assess worth of asset
- Calculate the single loss expectance
  - SLE = asset value * exposure factor
  - Exposure factor = % loss from exploitation
- Calculate Annualized loss expectancy
  - ALE = SLE * ARO (annualized rate of occurrence)

Cost Benefit Analysis Formula

- CBA = ALE (prior) – ALE (post) – ACS
  - ACS – annualized cost of the safeguard

Benchmarking

- Process of seeking out and studying the practices used in other organizations that produce results that you would like to duplicate in your organization
- Metrics
  - Number of successful attacks, staff-hours spent of systems protection, dollars spent on protection, number of security personnel, estimated value of info lost in attacks, loss in productivity hours
- Performance Gap

Baselining

- “ value of profile of a performance metric against which changes in the performance metric can be usefully compared”
- Analysis of measures against established standards

KEY

- “the goal of information security is not to bring residual risk to zero; it is to bring residual risk into line with an organization’s comfort zone or risk appetite”