Risk Management

Terminology Review (1)

- **System:** Collection of hardware, software, data, procedures, networks, people, etc. that "belong together"
- **Vulnerability**, **exploit, threat**, **threat agent**
- **Victim impact (or cost):** What happens to victim as the result of a successful attack
  - Damaged reputation
  - Lost sales
  - Replacement cost
  - Recovery cost (e.g., reinstall OS and applications)
  - Not limited to $$$

Terminology Review (2)

- **Attacker benefit:** What attacker gains from successful attack, e.g., $$, status in 1337 h4x0r underground, spreading political message by website defacement, etc.
- **Attacker cost:** What attacker "spends" to launch attack
  - Not limited to successful attacks
  - Not limited to $: could include special equipment, software, time, expertise, probability of getting caught and penalized
- **Risk:** Product of likelihood and magnitude of loss (when "bad things" happen)

Introduction

- **Risk management:** process of identifying and controlling risks facing an organization
  - **Risk identification:** process of examining an org.'s current IT security situation
  - **Risk control:** applying controls to reduce risks to org.'s data and information systems

Overview: Risk Management

- “If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.” – Sun Tzu, *The Art of War*
- This entails:
  - Knowing yourself: identifying and understanding existing information, systems in organization
  - Knowing the enemy: identifying and understanding threats facing org.

Risk Identification

- **Assets:** Anything that "has value" to organization
  - Includes people, data, computers, …
  - Attackers will target these (for various reasons)
- Risk management: identifying org.'s assets and threats to them (including vulnerabilities)
- Risk identification: need to specify org.'s assets, assessing their value

Identifying and Valuing Assets

- "It's all about the bookkeeping":
  - People: Who works for the organization?
  - Procedures: How do employees access data?
  - Data: What data does the org. store and process?
  - Hardware: What computer hardware does org use?
  - Software, networks: Same questions
- Assets are then classified and categorized
  - Business-critical? Moderate? Irrevelevant?
  - Database systems can help keep track of "stuff" (e.g., using inventory barcodes)

Classifying Info. Syst. Components (Table 4-1)

TABLE 4-1 Categorizing the Components of an Information System

Traditional system components	SecSDLC and risk management system components	
People	Employees	Trusted employees Other staff
	Nonemployees	People at trusted organizations Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive 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

Identification: People, Procedures, and Data

- Harder to track people, documentation, data than physical hardware, software licenses
- People with experience should do so
- Record assets via reliable data storage system

Questions

- What information should we record for:
  - People?
  - Business processes?
  - Data?
- What tools could we use to do so?
- How should a company manage the process of identifying

Hardware, Software, and Network Asset Identification

- What information attributes to track depends on:
  - Needs of organization/risk management efforts
  - Management needs of information security/information technology communities
- Asset attributes to be considered are: name; IP address; MAC address; element type; serial number; manufacturer name; model/part number; software version; physical or logical location; controlling entity

Information Classification

- Many organizations have data classification schemes (e.g., confidential, internal, public)
- Info. classification approach: specific categories
  - Requirements:
    - Each category has specific meaning
    - Categories must "span the gamut" of info. sensitivity levels
    - Categories must not overlap
  - Need to determine info. protection priorities
  - Table metaphor: category columns, info. rows

Information Valuation

- Info. has varying levels of importance
- What information:
  - is most critical to organization's success?
  - generates the most revenue/profitability?
  - would be most expensive to replace or protect?
  - would be the most embarrassing or cause greatest liability if revealed?
- How would you suggest valuing information? How often should we repeat valuation process?

Data Classification and Management

- Military classification:
  - Top Secret
  - Secret
  - Classified/Internal use only
  - Public
- Elaborate schemes: overkill for some orgs?

Threat Identification

- Security budgets limited; we can only focus on practical threats
- Threat assessment:
  - Which threats present danger to assets?
  - Which threats are the most dangerous to info.?
  - How much would it cost to recover from attack?
  - Which threat requires the most money to prevent?

Security Threats (Table 4.1)

Threat Category	Examples
Acts of human error or failure	***Accidents, employee mistakes***
Intellectual property compromise	Piracy, copyright infringement
Deliberate espionage or trespass	Unauthorized access, data collection
Deliberate information extortion	Blackmail of info. disclosure
Deliberate sabotage or vandalism	Destruction of systems or info.
Deliberate theft	Illegally taking equipment or info.
Deliberate software attacks	***Viruses, worms, denial of service***
Forces of nature	Fires, floods, earthquakes
Deviations in service from providers	Power and Internet provider issues
Technological hardware failures	Equipment failure
Technological software failures	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Vulnerability Identification

- ***Vulnerability:*** specific approach threat agents exploit to attack valuable information
- Questions to ask:
  - How could a threat be carried out?
  - What are the organization's assets?
  - What are the org.'s vulnerabilities?
- Recommendation: assemble people from diverse backgrounds in org., brainstorming meeting rounds
- Result of this process: list of assets, their vulnerabilities

Risk Assessment Worksheet

Asset	Asset Value ($)	Vuln.	Loss From Attack ($)	Probability of Vuln.	Expected Loss	Risk Ranking
Sensitive data	1,000,000	Disclosure	10,000,000	0.8	8,000,000	High
		Alien attack	100,000,000	0.000001	1,000	Low
Asset 1	…	…	…	…	…	…
Asset 2	…	…	…	…	…	…
…	…	…	…	…	…	…

- Actual worksheet varies for each organization
- Sort worksheet based on expected loss (high to low)
- Worksheet: input for risk control process

Risk Control

- Once ranked risk worksheet complete, choose one of four strategies to control each risk:
  - Apply safeguards (**avoidance**)
  - Transfer the risk (**transference**)
  - Reduce impact (**mitigation**)
  - Understand consequences and accept risk (**acceptance**)
- **Residual risk:** risk "left over" after identification and control

Avoidance

- Attempts to prevent vulnerability exploitation
- Preferred approach; techniques include:
  - Removing vulnerabilities
  - Limiting access to assets
  - Applying safeguards
- Three common methods of risk avoidance:
  - Impose policy
  - Educate people
  - Apply technology

Transference

- Shift risk to other assets, processes, or companies
- If lacking, organization should hire expert individuals, firms regarding security management
- Org. then transfers risk associated with IT mgmt. to another org. experienced in dealing with risks
- Residual risk: What happens if this org. hacked?

Mitigation

- Attempts to reduce impact of vulnerability exploitation via planning, preparation
- Approach includes three types of plans:
  - Incident response plan (IRP): What actions to take if there's an incident in progress?
  - Disaster recovery plan (DRP): Most common procedure
  - Business continuity plan (BCP): What to do if catastrophe strikes the organization?

Acceptance

- Doing nothing to protect a vulnerability, accepting outcome of its exploitation
- Valid only when some function, service, information, or asset does not justify protection cost
- Risk appetite: degree to which organization will accept risk as trade-off vs. cost of controls

Selecting a Risk Control Strategy

- Level of threat and value of asset play major role in selection of strategy
- Rules of thumb that we can apply:
  - A vulnerability exists
  - Attackers can exploit a vulnerability
  - Attacker's cost is less than potential gain
  - Substantial potential loss to organization

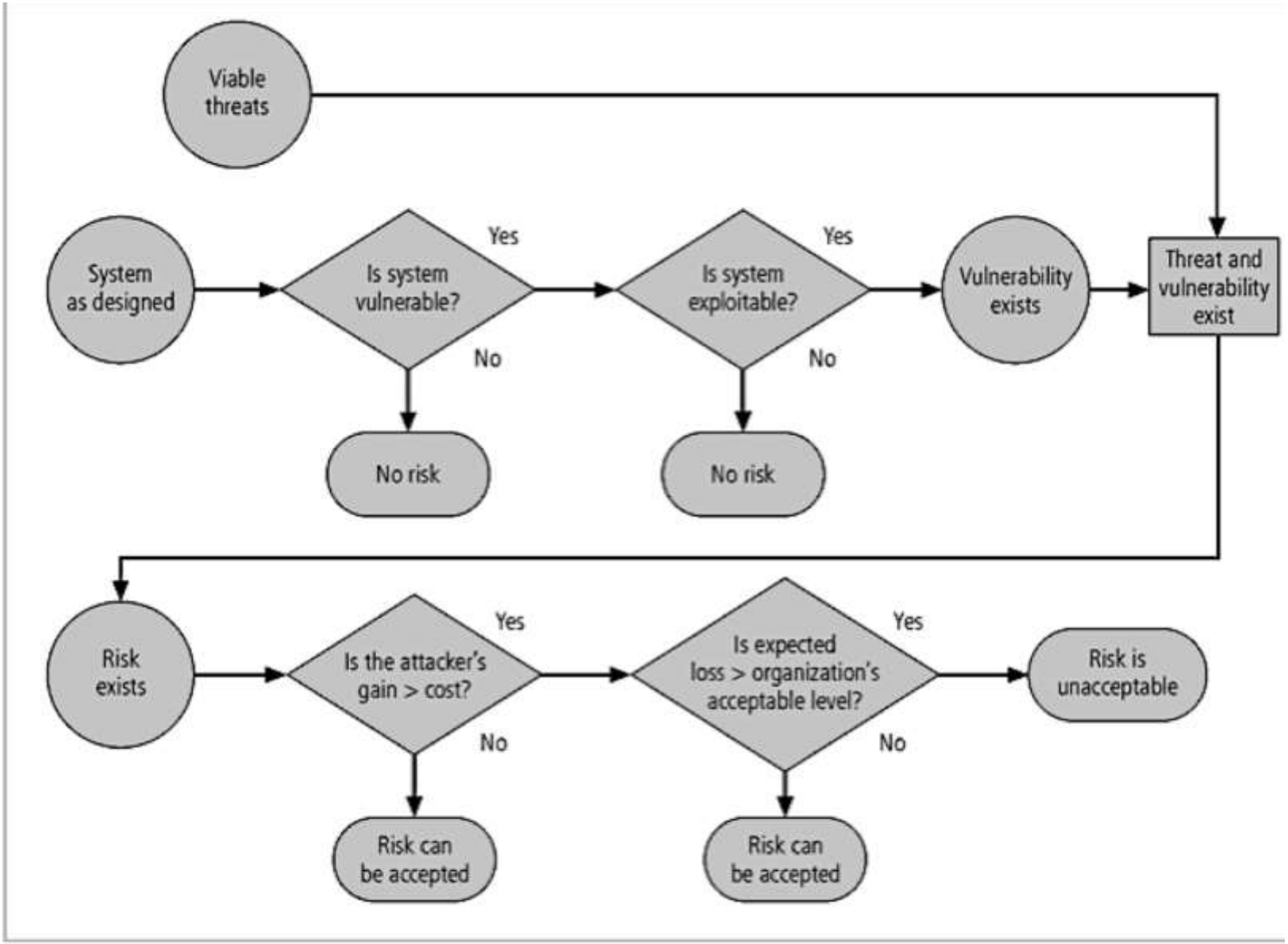

FIGURE 5-2 Risk Handling Decision Points[7]

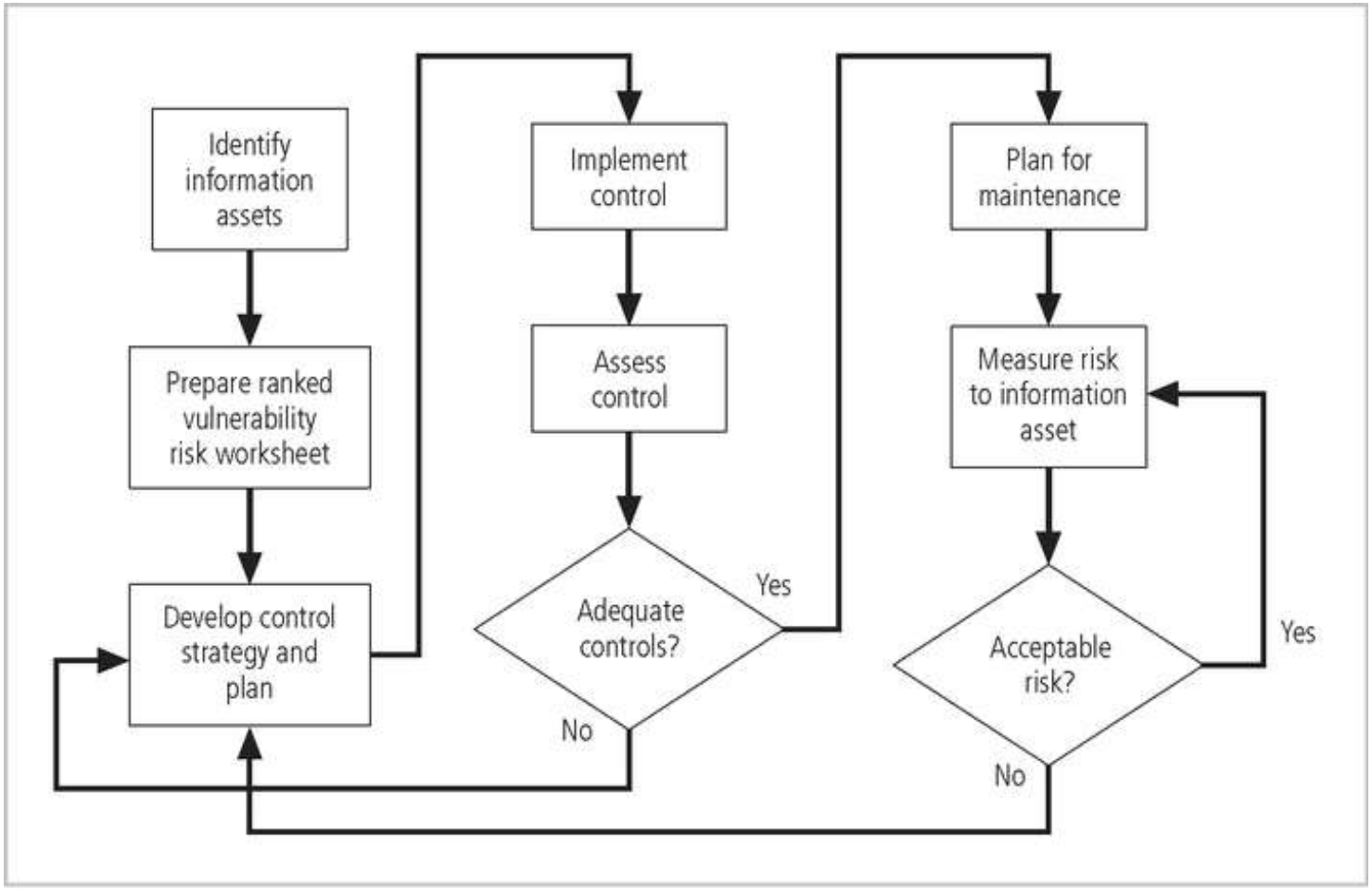

FIGURE 5-3 Risk Control Cycle[8]

Cost-Benefit Analysis (CBA) (1)

- Most common approach: economic feasibility of info. security controls
- CBA: first value assets to be protected, loss if they are compromised
- Formal process documenting this: cost-benefit analysis
- Cost of controls impacted by:
  - Costs: Development, implementation, maintenance, …
  - Training fees
- Benefit: value an organization realizes using controls to prevent losses from vulnerability
- Asset valuation: process of assigning monetary value to each piece of information (many parts)

Cost Benefit Analysis (CBA) (2)

- SLE: Single Loss Expectancy ($$)
- ARO: Annualized Rate of Occurrence (# times/yr.)
- ALE: Annualized Loss Expectancy = SLE × ARO ($$/yr)
- ACS: Annualized Cost of Safeguard ($$/year)
- CBA = $ALE_{prior} - ALE_{post} - ACS$ ($$/year)
  - If CBA is positive, that's good
  - If CBA is negative, spend more for protection than expected loss
  - Higher CBA is more efficient
- Problems:
  - "Garbage in garbage out" statistics
  - We don't know how often some events occur (or the unknown)
  - *Silo effect:* focus on specific systems, miss common controls

Benchmarking (1)

- Alternative approach to risk management: study practices in other organizations that your org. wants to duplicate
- One of two measures typically used to compare practices: metrics-based and process-based
- Benchmarking standards:
  - Due care: Show your org.'s security measures are similar to those of prudent org. (similar circumstances)
  - Due diligence: Show org. maintains security measures

Benchmarking (2)

- Best business practices: security efforts that provide a superior level protection of information
- When considering best practices for adoption in an organization, consider:
  - Does org. resemble target org. with best practice?
  - Are resources at hand similar?
  - Is org. in a similar threat environment?

Problems with Benchmarking and Best Practices

- Organizations don’t talk to each other
- No two orgs. are identical
- Best practices are a moving target
- Knowing recent events in security industry (benchmarking) may not prepare for future

Summary (1)

- Risk identification: process of examining and documenting risk present in information systems
  - Risk management strategy enables identification, classification, and prioritization of organization's information assets
  - Residual risk: risk that remains to the information asset even after the existing control is applied
- Risk control: process of protecting confidentiality, integrity, and availability of aspects of org.'s information system

Summary (2)

- Risk control: four strategies are used to control risks that result from vulnerabilities:
  - Apply safeguards (avoidance)
  - Transfer the risk (transference)
  - Reduce impact (mitigation)
  - Understand consequences and accept risk (acceptance)