

Information Systems



Chapter 5

Risk Management and Risk Analysis

-Sanket Mohan Pandhare



Introduction

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



An Overview of Risk Management

- Know yourself: identify, examine, and understand the information and systems ***currently in place***
- Know the enemy: identify, examine, and understand threats ***facing the organization***



Cont.

- Assets are targets of various threats and threat agents
- Risk management involves identifying organization's assets and identifying threats/vulnerabilities
- Risk identification begins with identifying organization's assets and assessing their value



Asset Identification and Valuation

- Iterative process; begins with identification of assets, including all elements of an organization's system (people, procedures, data and information, software, hardware, networking)
- Assets are then classified and categorized



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 |

People, Procedures, and Data Asset Identification



- Human resources, documentation, and data information assets are more difficult to identify
- People with knowledge, experience, and good judgment should be assigned this task
- These assets should be recorded using reliable data-handling process

People, Procedures, and Data Asset Identification (continued)



- Asset attributes for people: position name/number/ID; supervisor; security clearance level; special skills
- Asset attributes for procedures: description; intended purpose; what elements it is tied to; storage location for reference; storage location for update
- Asset attributes for data: classification; owner/creator/manager; data structure size; data structure used; online/offline; location; backup procedures employed

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

Data Classification and Management



- Variety of classification schemes used by corporate and military organizations
- Information owners responsible for classifying their information assets
- Information classifications must be reviewed periodically
- Most organizations do not need detailed level of classification used by military or federal agencies; however, organizations may need to classify data to provide protection



Threat Identification

- Realistic threats need investigation; unimportant threats are set aside
- Threat assessment:
 - Which threats present danger to assets?
 - Which threats represent the most danger to information?
 - How much would it cost to recover from attack?
 - Which threat requires greatest expenditure to prevent?



TABLE 4-3 Threats to Information Security

| Threat | Example |
|--|--|
| Act of human error or failure | Accidents, employee mistakes |
| Compromises to intellectual property | Piracy, copyright infringement |
| Deliberate acts of espionage or trespass | Unauthorized access and data collection |
| Deliberate acts of information extortion | Blackmail for information disclosure |
| Deliberate acts of sabotage or vandalism | Destruction of systems or information |
| Deliberate acts of theft | Illegal confiscation of equipment or information |
| Deliberate software attacks | Viruses, worms, macros, denial of service |
| Forces of nature | Fire, flood, earthquake, lightning |
| Quality of service deviations from service providers | Power and WAN quality of service issues |
| Technical hardware failures or errors | Equipment failure |
| Technical software failures or errors | Bugs, code problems, unknown loopholes |
| Technological obsolescence | Antiquated or outdated technologies |

©2003 ACM, Inc., Included here by permission.



Vulnerability Identification

- Specific avenues threat agents can exploit to attack an information asset are called vulnerabilities
- Examine how each threat could be perpetrated and list organization's assets and vulnerabilities
- Process works best when people with diverse backgrounds within organization work iteratively in a series of brainstorming sessions
- At end of risk identification process, list of assets and their vulnerabilities is achieved



Risk Assessment

- Risk assessment evaluates the relative risk for each vulnerability
- Assigns a risk rating or score to each information asset



Documenting the Results of Risk Assessment

- Final summary comprised in ranked vulnerability risk worksheet
- Worksheet details asset, asset impact, vulnerability, vulnerability likelihood, and risk-rating factor
- Ranked vulnerability risk worksheet is initial working document for next step in risk management process: assessing and controlling risk



Risk Control

- Once ranked vulnerability risk worksheet complete, must 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)



Avoidance

- Attempts to prevent exploitation of the vulnerability
- Preferred approach; accomplished through countering threats, removing asset vulnerabilities, limiting asset access, and adding protective safeguards
- Three common methods of risk avoidance:
 - Application of policy
 - Training and education
 - Applying technology



Transference

- Control approach that attempts to shift risk to other assets, processes, or organizations
- If lacking, organization should hire individuals/firms that provide security management and administration expertise
- Organization may then transfer risk associated with management of complex systems to another organization experienced in dealing with those risks



Mitigation

- Attempts to reduce impact of vulnerability exploitation through planning and preparation
- Approach includes three types of plans:
 - Incident response plan (IRP)
 - Disaster recovery plan (DRP)
 - Business continuity plan (BCP)



Mitigation (continued)

- DRP is most common mitigation procedure
- The actions to take while incident is in progress is defined in IRP
- BCP encompasses continuation of business activities if catastrophic event occurs



Acceptance

- Doing nothing to protect a vulnerability and accepting the outcome of its exploitation
- Valid only when the particular function, service, information, or asset does not justify cost of protection
- Risk appetite describes the degree to which organization is willing to accept risk as trade-off to the expense of applying controls

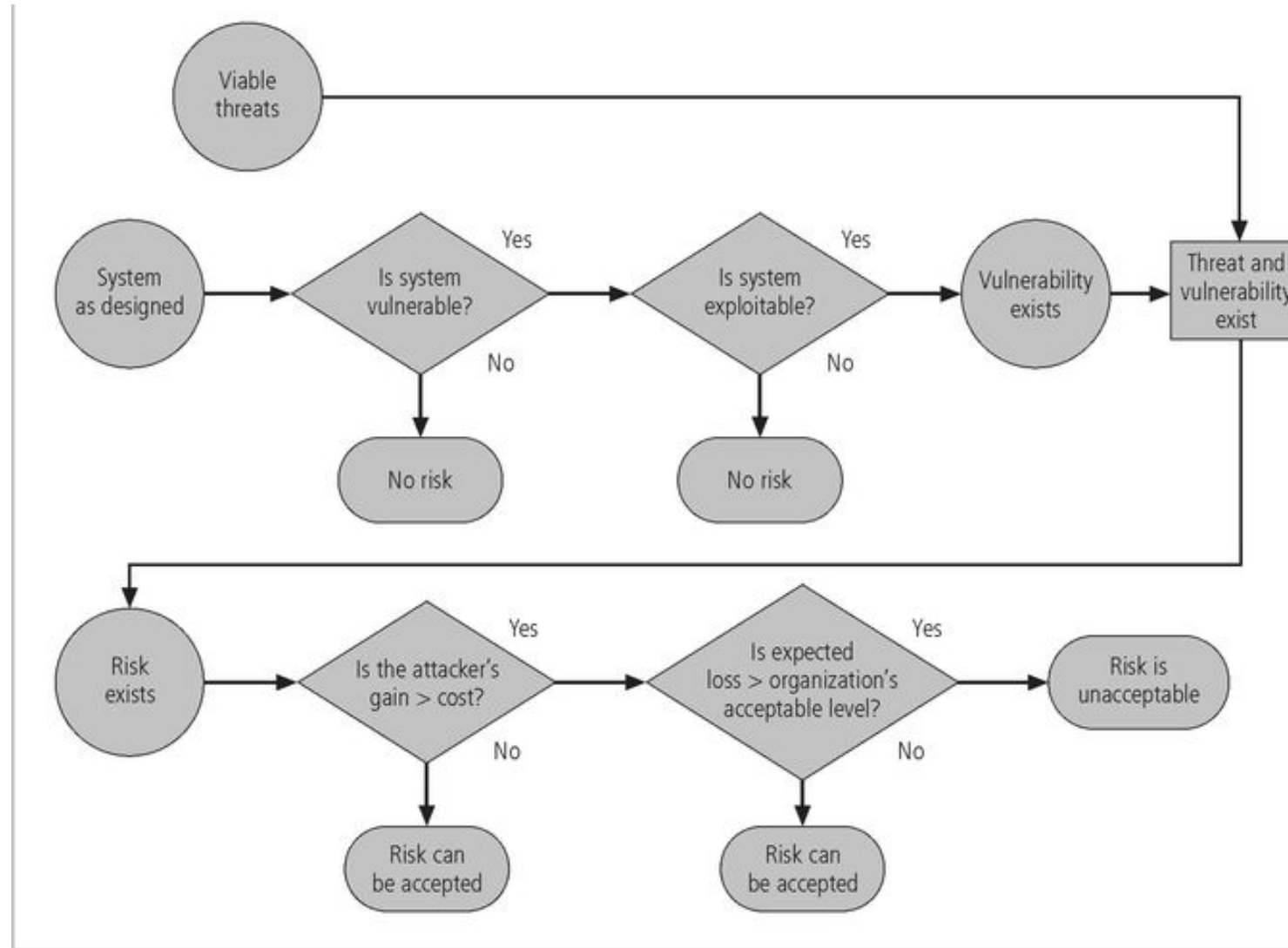


FIGURE 5-2 Risk Handling Decision Points⁷



Cost Benefit Analysis (CBA)

- Most common approach for information security controls is economic feasibility of implementation
- CBA is begun by evaluating worth of assets to be protected and the loss in value if those assets are compromised
- The formal process to document this is called cost benefit analysis or economic feasibility study



Cost Benefit Analysis (CBA) (continued)

- Items that impact cost of a control or safeguard include: cost of development; training fees; implementation cost; service costs; cost of maintenance
- Benefit is the value an organization realizes by using controls to prevent losses associated with a vulnerability
- Asset valuation is process of assigning financial value or worth to each information asset; there are many components to asset valuation



Benchmarking

- An alternative approach to risk management
- Benchmarking is process of seeking out and studying practices in other organizations that one's own organization desires to duplicate
- One of two measures typically used to compare practices:
 - Metrics-based measures
 - Process-based measures

Benchmarking (continued)



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



Problems with Applying Benchmarking and Best Practices

- Organizations don't talk to each other (biggest problem)
- No two organizations are identical
- Knowing what was going on in information security industry in recent years through benchmarking doesn't necessarily prepare for what's next



Summary

- Risk identification: formal process of examining and documenting risk present in information systems
- Risk control: process of taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of components in organization's information system
- Risk identification
 - A 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

Summary



- 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)