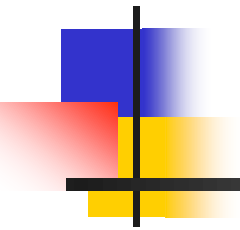
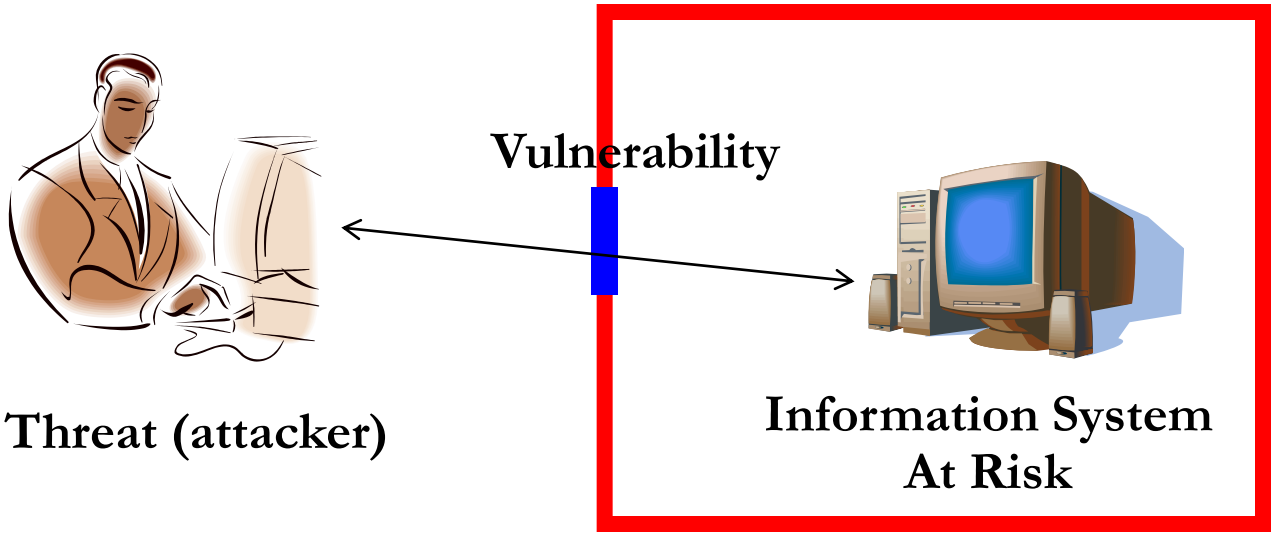


Risk Management

Professor Stephen S. Yau

What Is a Risk?



- Concepts revisit
  - A *threat* is a ***potential occurrence*** that can have an ***undesirable effect*** on the system assets or resources
  - A *vulnerability* is a ***weakness*** that makes a threat to possibly occur
- A *risk* is a ***potential negative event*** that may affect the successful operations of a system
  - A risk is *not necessarily* an ongoing problem

Common Threats

- Acts of human error or failure
- Compromises to intellectual property
- Deliberate acts of trespass
- Deliberate acts of information extortion
- Deliberate acts of sabotage or vandalism
- Deliberate acts of theft
- Deliberate software attacks
- Forces of nature
- Deviations in quality of service
- Technical hardware failure or errors
- Technical software failures or errors
- Technological obsolescence

Vulnerability Category

- Probabilistic vulnerabilities
  - Caused by hardware failures, human actions and information problems in the operational environment
- Algorithmic vulnerabilities
  - Caused by design and implementation errors introduced during system development [including both software and hardware]

Identification of Possible Risks

- What is at risk?
  - Product design documents
  - Customer information
  - Company's future plan
  - …
- For each threat, *what* and *where* and other *factors*?
  - Who? (competitors, foreign agents, hackers)
  - Motivation? (national security, money, fame, "fun")
  - Target? (access confidential data, change data, deface…)
  - Capabilities? (intellect, equipment, money)
- What vulnerabilities can be exploited?
  - Technology?
  - Process?
  - Network?
  - People?

Components of Information System

Traditional System Components	Risk Management	System Components
People	Employees	Trusted employees (including clearance) / Other Staff
	Nonemployees	People at trusted organizations/Others
Procedures	IT & business procedures	For handling sensitive info. / For handling non-sensitive info.
Information	Information	Transmission, Processing, Storage
Software	Software	Applications, Operating systems, Security components
Hardware	System devices and peripherals	Systems and peripherals, Security devices
Network	Network components	Intranet components, Internet or DMZ components

Cost/Benefit Analysis

After identifying possible risks, cost/benefit analysis is needed for the following reasons:

- Infeasible or sometimes impossible to implement a perfect secure systems
- Cost/benefit analysis helps identify risks which will most likely occur, and cause severe damages if occur
- Acceptable risks: Some risks are always there (***residual risk***). But they highly unlikely become problems; or they can easily be contained and solved if becoming problems.
- Cost/benefit analysis is needed to allocate limited resources (financial, people, system) to most needed areas

Risk Analysis

- A process to systematically identify assets, threats, and (potential) vulnerabilities in a system, and to address:
  - Which threats present danger to your assets?
  - Which threats represent the most danger to organizations' sensitive information?
  - How much would it cost to recover from attack?
  - Which threat requires greatest resources to prevent?
  - Which of the above questions for each asset is most important to protection of organizations' information?
- Should be a continuous process over the life cycle of a system (design, implementation, testing, deployment, update and termination)

Risk Analysis (cont.)

Risk rating = V*L*(1-P+U),

where

- *V*: The value of the information asset
- *L*: The likelihood of the occurrence of a vulnerability
- *P*: The percentage of the risk mitigated by current controls
- *U*: The uncertainty of current knowledge of the vulnerability

Risk Analysis Example

- Information asset A has one vulnerability #1
  - The value of A is 50
  - The likelihood of the vulnerability is 0.1
  - Has no control (not addressed in risk management)
  - Assumptions and data are estimated 90% accurate
- Information asset B has two vulnerabilities #2 and #3
  - The value of B is 100
  - The likelihood of vulnerabilities #2 and #3 are 0.5 and 0.1
  - Current control addresses 50% of the risk of vulnerability #2, and 0% of the risk of vulnerability #3.
  - Assumptions and data are estimated 80% accurate

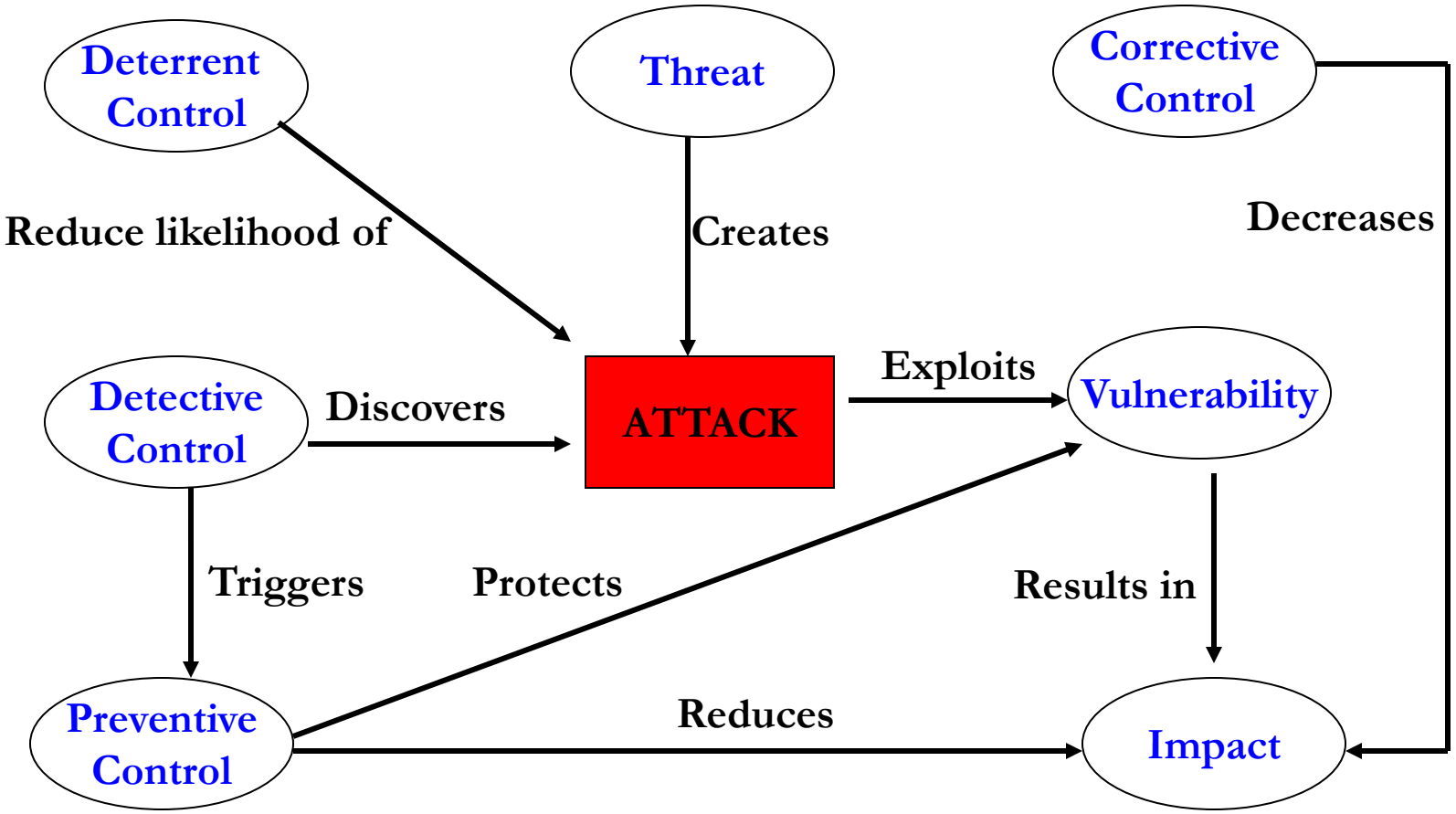
Controls

- Countermeasures for vulnerabilities
  - ***Deterrent controls*** discourage violation and reduce likelihood of deliberate attacks
    - Sanctions built into organizational policies, punishments imposed by legislation
  - ***Preventive controls*** stop attempts to exploit vulnerabilities
    - Segregation of duties, proper authorization, adequate documents, proper record keeping, physical controls

Controls (cont.)

- ***Detective controls*** discover attacks and trigger preventive or corrective controls
  - Firewall logs, inventory counts, input edit checks, checksums, and message digests
- ***Corrective controls*** reduce the effect of an attack
  - Virus quarantine, firewall rule reconfiguration
- ***Recovery controls*** restore lost computer resources or capabilities from security violations
  - Business continuity planning, disaster recovery plans, backups

A Model of Risk Analysis Process



Risk Management

- Concerned with ***preventing risks from becoming problems***
- How to deal with risks identified in the risk analysis?
  - Old philosophy: ***risk avoidance***
    - Do whatever you can to avoid risks
  - New philosophy: ***risk management***
    - Understand risks
    - Deal with them in an appropriate, cost-effective manner

Risk Management (cont.)

- Choices for each risk
  - **Risk acceptance:** tolerate those risks with low impact or rare occurrence
  - **Risk reduction** (also called **risk mitigation**)
  - **Risk transfer** (to another entity): let others handle the risk
- Typically use a combination of acceptance, reduction, and transfer for different risks

Risk Acceptance

- ***Risk acceptance*** can be established after the organization has done the following:
  - Determine the level of each identified risk
  - Assess the probability of each type of potential attacks
  - Estimate potential damage from each type of attacks
  - Perform cost-benefit analysis on reducing each type of risks
  - Evaluate controls using each appropriate type of feasibility
  - Decide that the particular function, service, information, or asset did not justify the cost for protection

Mitigation

- ***Mitigation***: Attempting to ***reduce impact*** caused by exploitation of vulnerability through ***planning and preparation***
  - ***Incident Response Plan***: Actions and organization takes during incidents (attacks)
  - ***Disaster Recovery Plan***: Preparation for recovery if a disaster occurs; strategies to limit losses before and during disaster; stepwise instructions to regain normalcy
  - ***Business Continuity Plan***: Steps to ensure continuation of overall business when the scale of a disaster exceeds the Disaster Recovery Plan's ability to restore operations

Examples

Choices for risk	Car theft	Hacker break-in
Acceptance	Deductibles on car insurance	Minimal security (turn off computers not in use)
Reduction	Locks, alarms, garage, etc.	Strong security mechanisms (firewall, encryption, etc.)
Transfer	Car insurance covering theft	Rely on Internet Service Provider (ISP) to provide security guarantees

Some Risk Management Strategies

- ***When a vulnerability exists:*** Implementation security controls to reduce likelihood of a vulnerability being exercised.
- ***When a vulnerability can be exploited:*** Apply layered protections, architectural designs, and administrative controls to minimize the risk or prevent occurrence.
- ***When attacker's cost is less than his potential gain:*** Apply protection to increase attack's cost.
- ***When potential loss is substantial:*** Apply design principles, architectural designs, and technical and nontechnical protections to limit extent of attack, thereby reducing potential loss.

Risk Management Process

- ***Step 1:*** System characterization
  - ***Input***: hardware, software, system interfaces, system mission, people, data information
  - ***Output***: system boundary, system functions, system and data criticality and sensitivity
- ***Step 2:*** Threat identification
  - ***Input***: attack history, data from intelligence agencies or mass media
  - ***Output***: threat statement

Risk Management Process (cont.)

- ***Step 3:*** Vulnerability identification
  - ***Input***: prior risk assessment reports, audit comments, security requirements, security test results
  - ***Output***: list of potential vulnerabilities
- ***Step 4:*** Control analysis
  - ***Input***: current controls, planned controls
  - ***Output***: evaluation results of current and planned controls

Risk Management Process (cont.)

- ***Step 5:*** Likelihood determination
  - ***Input***: threat-source motivation, threat capacity, nature of vulnerability, current controls
  - ***Output***: likelihood rating
- ***Step 6:*** Impact analysis
  - ***Input***: mission impact analysis, asset criticality assessment, data criticality and sensitivity
  - ***Output***: impact rating
- ***Step 7:*** Risk determination
  - ***Input:*** likelihood of threat exploitation, magnitude of impact, adequacy of planned or current controls
  - ***Output***: risks and associated risk levels

Risk Management Process (cont.)

- ***Step 8:*** Control recommendations
  - ***Output***: recommended controls
- ***Step 9:*** Results documentation
  - ***Output***: A set of documents, including risk identification, assessment, cost-effective evaluation, suggested control list.

A well documented risk management process at one phase, which is also the starting point for the analysis at the next phase

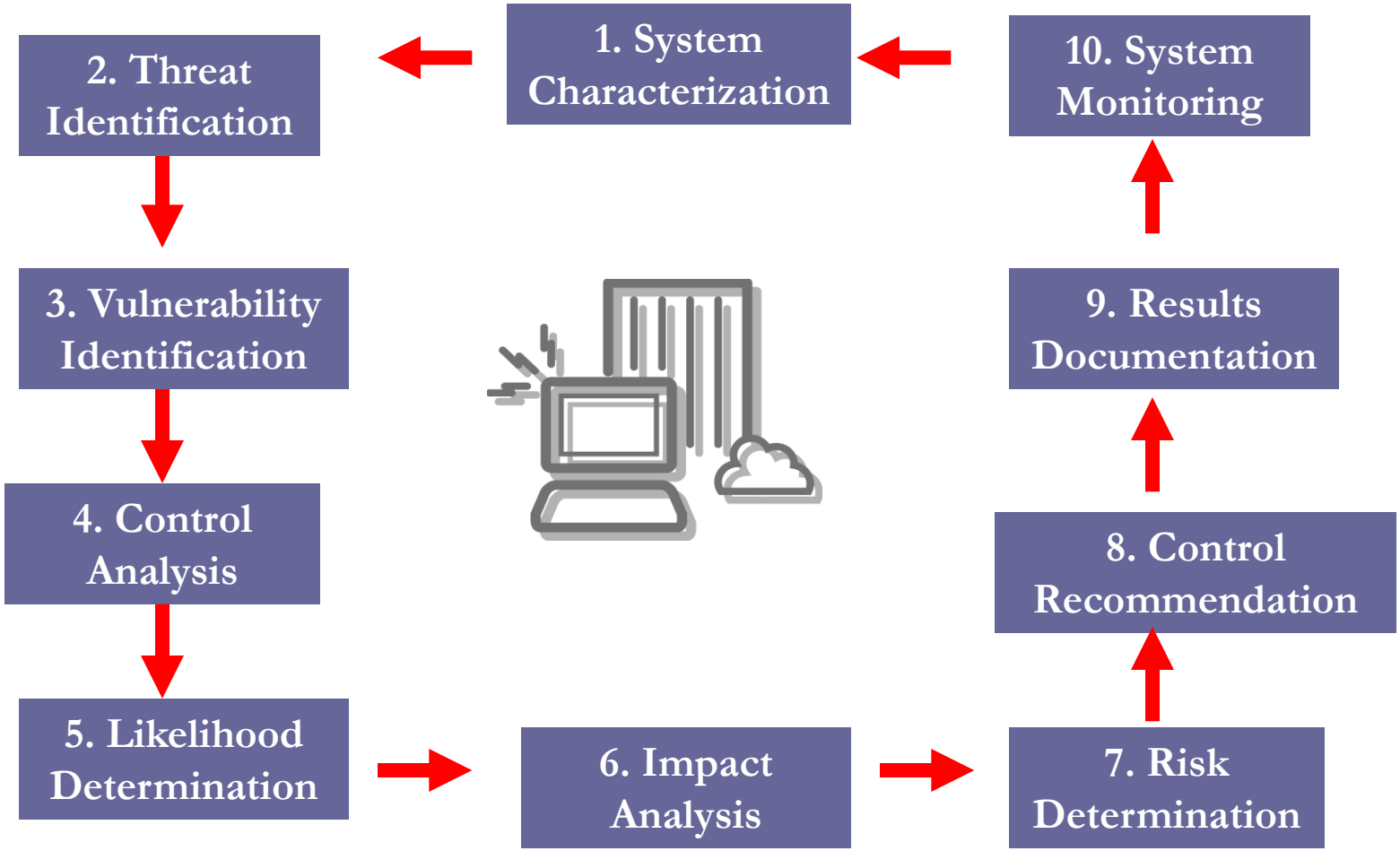
Risk Management Process (cont.)

- ***Step 10:*** System monitoring:
  - Whether system configuration has changed: New hardware installed, software updates, mission goal changed, etc.
  - Performance of controls: How many possible attacks have been prevented by controls; any failures or unwanted outcome, etc.

Restart the whole process from Step 1 again:

- Periodically as part of system maintenance procedure
- When system configuration is changed, it may generate some new risks not covered during the last risk management process
- When some controls fail to prevent the risk from turning into attacks

Risk Management Process (cont.)



References

- Michael E. Whitman, Herbert J. Mattord , *Principles of Information Security*, Course Technology, 2011
- Risk Management Guide for Information Technology Systems, July 2002. Available at: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- Mark Stamp, *Information Security: Principles and Practice*, Wiley, May 2011, 606 pages, ISBN-10 0470626399
- Evan Wheeler, *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*, Syngress, May 2011, 360 pages, ISBN-10 1597496154
- Te-Shun Chou, *Information Assurance and Security Technologies for Risk Assessment and Threat Management: Advances (Premier Reference Source)*, IGI Global, December 2011, 371 pages, ISBN-10 1613505078