SECURITY IN COMPUTING, FIFTH EDITION

Chapter 10: Management and Incidents

https://digitalguardian.com/blog/what-security-incident-management-cybersecurity-incident-management-process

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Chapter 10 Objectives

- Study the contents of a good security plan
- Learn to plan for business continuity and responding to incidents
- Outline the steps and best practices of risk analysis
- Learn to prepare for natural and human-caused disasters

Security Plan

- In the past, most computing was done on mainframe computers
- Data processing centers were responsible for protection
  - Implemented protection activities in the background
- Programmers and users were not responsible for the system security
  - Were not aware of protection needs and practices.

Security Plan

- With introduction of personal computers, security responsibility shifted to users
- However, many users are unaware with the risks
  - Do not take precautions or implement security measures
- Sensitive data may be accessed from laptops and mobile devices
  - Need to be protected

Security Plan

- Every organization using computers to create and store valuable assets should perform thorough and effective security planning.
- A **security plan** is a document that describes how an organization will address its security needs.
- The plan is subject to periodic review and revision as the organization's security needs change

Security Plan

- A security plan identifies and organizes the security activities for a computing system.
- The plan is both a description of the current situation and a map for improvement.
- It is both an official record of current security practices and a blueprint for orderly change to improve those practices.
- We discuss some of its contents in more detail in the following slides.

Contents of a Security Plan

- *Policy,* indicating the goals of a computer security effort and the willingness of the people involved to work to achieve those goals
- *Current state*, describing the status of security at the time of the plan
- *Requirements*, recommending ways to meet the security goals
- *Recommended controls*, mapping controls to the vulnerabilities identified in the policy and requirements

Contents of a Security Plan (cont.)

- *Accountability*, documenting who is responsible for each security activity
- *Timetable*, identifying when different security functions are to be done
- *Maintenance,* specifying a structure for periodically updating the security plan

Security Policy

- Overall organizational security policy:
  - A high-level statement of purpose and intent
  - Answers three essential questions:
    - Who should be allowed access?
    - To what system and organizational resources should access be allowed?
    - What types of access should each user be allowed for each resource?
- Security policies and plans often should also exist at the level of systems or groups of systems

Security Policy

- An organization-wide security policy can address users and systems only in the context of fairly general roles
  - Not specific enough for many purposes
- Organizations as a whole may be primarily focused on maintaining confidentiality of data
  - However, certain systems in the organization may rightfully focus on maintaining availability
    - as a top priority

Security Policy

- Should specify
  - The organization's security goals (e.g., define whether reliable service is a higher priority than preventing infiltration)
  - Where the responsibility for security lies (e.g., the security group or the user)
  - The organization's commitment to security (e.g., defines where the security group fits in the corporate structure)

Assessment of Current Security Status

- A risk analysis—a systemic investigation of the system, its environment, and what might go wrong—forms the basis for describing the current security state
- Defines the limits of responsibility for security
  - Which assets are to be protected
  - Who is responsible for protecting them
  - Who is excluded from responsibility
  - Boundaries of responsibility

Security Requirements

- Security requirements are functional or performance demands placed on a system to ensure a desired level of security
- Usually derived from organizational business needs, sometimes including compliance with mandates imposed from outside, such as government standards

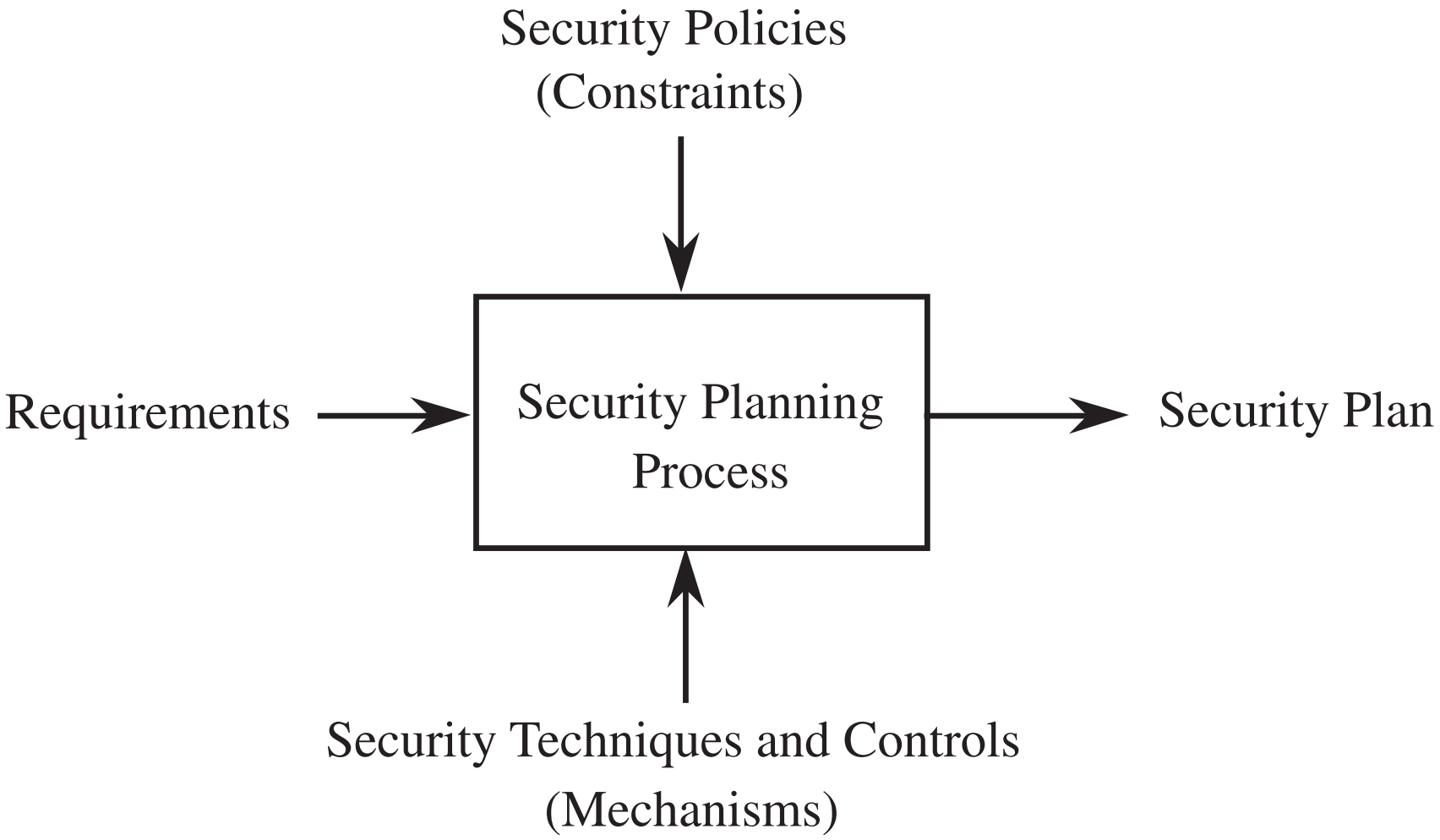
Requirements, Constraints and Controls

- **Requirements**:
  - functional or performance demands placed on a system to ensure a desired level of security
  - Requirements explain *what* should be accomplished, not *how*
    - Should always leave the implementation details to the designers
- **Constraint:**
  - An aspect of the security policy that constrains, circumscribes, or directs the implementation of the requirements

Requirements, Constraints and Controls

- **Control:**
  - An action, device, procedure, or technique that removes or reduces a vulnerability
  - The designers should select appropriate controls
    - such as tokens or encryption
  - The designers should balance security requirements with other system requirements
    - such as performance and reliability

Inputs to the Security Plan



Security Requirements

- Characteristics of good security requirements:
  - Correctness
  - Consistency
  - Completeness
  - Realism
  - Need
  - Verifiability
  - Traceability

Security Requirements

- *Correctness:* Are the requirements understandable? Are they stated without error?
- *Consistency:* Are there any conflicting or ambiguous requirements?
- *Completeness:* Are all possible situations addressed by the requirements?
- *Realism:* Is it possible to implement what the requirements mandate?

Security Requirements

- *Need:* Are the requirements unnecessarily restrictive?
- *Verifiability:* Can tests be written to demonstrate conclusively and objectively that the requirements have been met? Can the system or its functionality be measured in some way that will assess the degree to which the requirements are met?
- *Traceability:* Can each requirement be traced to the functions and data related to it so that changes in a requirement can lead to easy reevaluation?

Recommended Controls

- Security requirements describe system's needs
  - What should be protected
- Should also recommend the controls should be incorporated into the system
  - To meet these requirements
- Risks analysis can be created to map vulnerabilities to controls
  - Recommended controls will address implementation issues:
    - How will the system design meet the security requirements?

Responsibility for Implementation

- A section of the security plan will identify which people (roles) are responsible for implementing security requirements
- The plan makes explicit who is accountable should some requirement not be met or some vulnerability not be addressed
  - who is responsible for implementing controls when a new vulnerability is discovered or a new kind of asset is introduced
  - **No one responsible implies no action**

Who Is Responsible for Using Security?

- User asked to handle certain tasks:
  - Apply security patches, don't download unknown code, keep sensitive material private, change your password frequently
- can we expect people to use their computers securely?
  - when that is so hard to do?

Who Is Responsible for Using Security?

- According to Whitten [WHI99], user should be:
  - Made aware of the security of tasks they need to perform
  - Able to figure out how to perform those tasks successfully
  - Prevented from making dangerous errors
  - Sufficiently comfortable with the technology to continue using it

Who Is Responsible for Using Security?

- Many products not usable enough to provide effective security for most computer users
  - According to these guidelines
  - Security settings often hidden on a sub-sub-tab
    - written in highly technical jargon
- Need to make the interface consistent, informative, empowering, and error preventing

Responsibility for Implementation

- Common roles:
  - *Users* of personal computers or other devices may be responsible for the security of their own machines.
    - Alternatively, the security plan may designate one person or group to be coordinator of personal computer security.
  - *Project leaders* may be responsible for the security of data and computations.
  - *Managers* may be responsible for seeing that the people they supervise implement security measures.

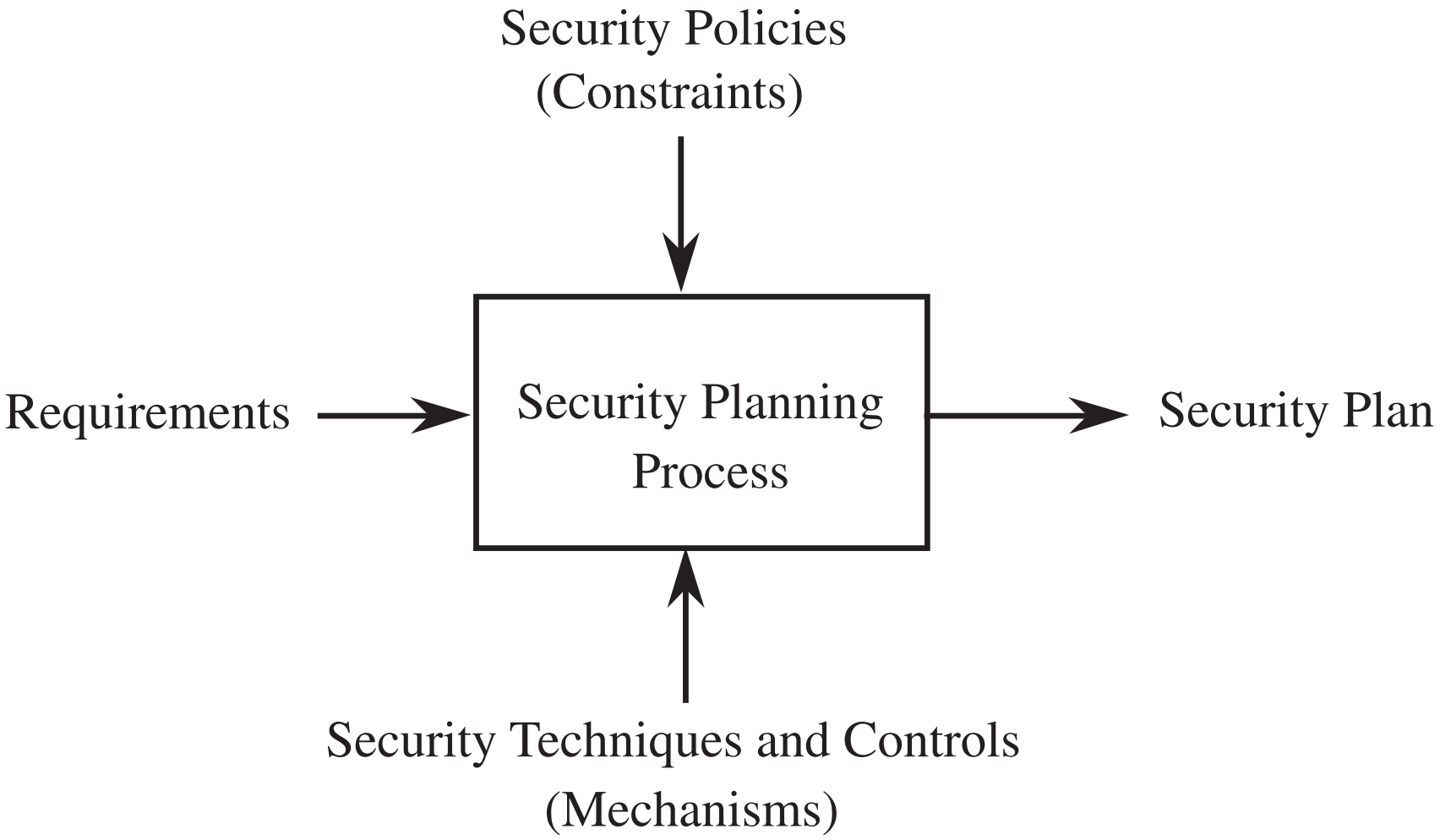
Responsibility for Implementation

- Common roles (cont.):
  - *Database administrators* may be responsible for the access to and integrity of data in their databases.
  - *Information officers* may be responsible for overseeing the creation and use of data
    - these officers may also be responsible for retention and proper disposal of data.
  - *Personnel staff members* may be responsible for security involving employees
    - for example, screening potential employees for trustworthiness and arranging security training programs.

Timetable and Plan Maintenance

- As a security plan cannot be implemented instantly, the plan should include a timetable of how and when the elements in it will be performed
- The plan should specify the order in which controls are to be implemented so that the most serious exposures are covered as soon as possible
- The plan must be extensible, as new equipment will be acquired, new connectivity requested, and new threats identified
  - The plan must include procedures for change and growth
  - The plan must include a schedule for periodic review

Inputs to the Security Plan



Security Planning Team Members

- Security planning touches every aspect of an organization and therefore requires participation well beyond the security group
- Members of the team should relate to the different aspects of computer security
  - Administration staff for OS and networks
  - Application programmers for program security measures
  - General physical security agents for physical security
  - Users' views for usability of the controls proposed

Security Planning Team Members

- Common security planning representation:
  - Computer hardware group
  - System administrators
  - Systems programmers
  - Applications programmers
  - Data entry personnel
  - Physical security personnel
  - Representative users

Assuring Commitment to a Security Plan

- A plan that has no organizational commitment collects dust on a shelf
- Three groups of people must contribute to making the plan a success:
  - The planning team must be sensitive to the needs of each group affected by the plan.
  - Those affected by the security recommendations must understand what the plan means
    - Way they will use the system and perform their business activities.
    - How what they do can affect other users and other systems.
  - Management must be committed to using and enforcing the security aspects of the system.

Business Continuity Planning

- A business continuity plan documents how a business will continue to function during or after a computer security incident
- Addresses situations having two characteristics:
  - *Catastrophic situations,* in which all or a major part of a computing capability is suddenly unavailable
  - *Long duration,* in which the outage is expected to last for so long that business will suffer

Business Continuity Planning

- Examples when such a plan will be helpful:
  - A company network is destroyed by a fire
  - Failure of a critical software component
    - Results in an unusable computing system
  - Electricity, telecommunication, network access failure
    - Abruptly, limits or completely stops activity of system
  - Flood
    - Preventing personnel from getting to operations system

Business Continuity Planning

- Specific tasks involve:
  - Assessing business impact
  - Developing a control strategy
  - Develop a strategy implementation plan

Continuity Planning Activities

- Assess the business impact of a crisis
  - What are the essential assets?
  - What could disrupt use of these assets?
- Develop a strategy to control impact
  - Investigate how the key assets can be safeguarded
- Develop and implement a plan for the strategy
  - Define:
    - Who is in charge when an incident occurs
    - What to do when an incident occurs
    - Who does what tasks when an incident occurs

Incident Response Plans

- A security incident response plan tells the staff how to deal with a security incident
- In contrast to a business continuity plan, the goal of incident response is handling the current security incident without direct regard for the business issues
- An incident response plan should
  - Define what constitutes an incident
  - Identify who is responsible for taking charge of the situation
  - Describe the plan of action

Incident Response Teams

- The response team is charged with responding to the incident. It may include
  - Director : The person in charge of the incident, who decides what actions to take
  - Technicians: People who perform the technical part of the response
  - Advisors: Legal, human resources, or public relations staff members as appropriate

Incident Response Teams

- Matters to consider when identifying a response team:
  - Legal issues
  - Preserving evidence
  - Records
  - Public relations

CSIRTs

- Computer Security Incident Response Teams (CSIRT) are teams trained and authorized to handle security incidents
- CSIRTs are closely related to, and often heavily overlap, Security Operations Centers (SOC)
  - SOC perform day-to-day monitoring of a network and may be the first to detect an incident

CSIRTs

- Responsibilities of a CSIRT include
  - Reporting: Receiving reports of suspected incidents and reporting as appropriate to senior management
  - Detection: Investigation to determine if an incident occurred
  - Triage: Immediate action to address urgent needs
  - Response: Coordination of effort to address all aspects in a manner appropriate to severity and time demands

CSIRTs

- Responsibilities of a CSIRT include (cont.)
  - Postmortem: Declaring the incident over and arranging to review the case to improve future response
  - Education: Preventing harm by advising on good security practices and disseminating lessons learned from past incidents

CSIRT Skills

- Collect, analyze, and preserve digital forensic evidence
- Analyze data to infer trends
- Analyze the source, impact, and structure of malicious code
- Help manage installations and networks by developing defenses such as signatures
- Perform penetration testing and vulnerability analysis
- Understand current technologies used in attacks

Risk Analysis

- Risk analysis is an organized process for identifying the most significant risks in a computing environment, determining the impact of those risks, and weighing the desirability of applying various controls against those risks
- A risk is a potential problem that the system or its users may experience

Risk Analysis

- Characteristics of a risk:
  - Associated loss (also known as a *risk impact*)
  - Likelihood of occurring
  - Degree to which we can change the outcome (risk control)
- We can theoretically quantify the effects of a risk, or risk exposure
  - by multiplying likelihood by risk impact
  - However, even though risks have likelihoods associated with them, those likelihoods, in the context of cybersecurity, are generally impossible to measure

Strategies for Dealing with Risk

- *Avoid* the risk by changing requirements for security or other system characteristics
- *Transfer* the risk by allocating the risk to other systems, people, organizations, or assets or by buying insurance to cover any financial loss should the risk become a reality
- *Assume* the risk by accepting it, controlling it with available resources, and preparing to deal with the loss if it occurs

Steps of a Risk Analysis

1. Identify assets.
2. Determine vulnerabilities.
3. Estimate likelihood of exploitation.
4. Compute expected annual loss.
5. Survey applicable controls and their costs.
6. Project annual savings of control.

Step 1: Identify Assets

- Hardware:
  - Processors, boards, keyboards, monitors, terminals, microcomputers, workstations,
  - Tape drives, printers, disks, disk drives,
  - Cables, connections, communications controllers, and communications media
- Software:
  - Source programs, object programs, purchased programs, in-house programs, utility programs
  - Operating systems, systems programs (such as compilers)
  - Maintenance diagnostic programs

Step 1: Identify Assets

- Data:
  - Data used during execution,
  - Stored data on various media
  - Printed data, archival data, update logs, and audit records
- People:
  - Skilled staff needed to run the computing system or specific programs
  - Support personnel such as guards

Step 1: Identify Assets

- Documentation:
  - On programs, hardware, systems, administrative procedures, and the entire system
- Supplies:
  - Paper, forms, laser cartridges, recordable media, and printer ink
  - Power, heating and cooling
  - Necessary buildings or shelter

Step 1: Identify Assets

- Reputation: Company image
- Availability:
  - Ability to do business, ability to resume business rapidly and efficiently after an incident

Step 2: Determine Vulnerabilities

Asset	Secrecy	Integrity	Availability
Hardware		overloaded destroyed tampered with	failed stolen destroyed unavailable
Software	stolen copied pirated	impaired by Trojan horse modified tampered with	deleted misplaced usage expired
Data	disclosed accessed by outsider inferred	damaged - software error - hardware error - user error	deleted misplaced destroyed
People			quit retired terminated on vacation
Documentation			lost stolen destroyed
Supplies			lost stolen damaged

Step 2: Determine Vulnerabilities

- This is an example of a matrix mapping vulnerabilities to assets
- In real life, the matrix would be much longer and include much more specific assets
- Numerous vulnerability types can apply broadly to a class of assets
  - however, broad categories are useful and help identify organization-wide concerns.

Step 2: Determine Vulnerabilities

- In considering the contents of each matrix entry, we can ask some helpful questions:
  - What are the effects of unintentional errors?
    - Consider typing the wrong command, entering the wrong data, using the wrong data item, discarding the wrong listing, and disposing of output insecurely.
  - What are the effects of willfully malicious insiders?
    - Consider disgruntled employees, bribery, and curious browsers.

Step 2: Determine Vulnerabilities

- In considering the contents of each matrix entry, we can ask some helpful questions (cont.):
  - What are the effects of outsiders?
    - Consider network access, remote access, hackers, people walking through the building, people snooping at coffee shops, and people sifting through the trash.
  - What are the effects of natural and physical disasters?
    - Consider fires, storms, floods, power outages, and component failures.

Step 3: Estimate Likelihood of Exploitation

- Because it is impossible to know all of a system's vulnerabilities or all the ways those vulnerabilities can be exploited, is also impossible to accurately assess likelihood of exploitation
- Possible approaches to estimation:
  - Apply frequency probability using observed data for a similar system
  - Use an analyst familiar with such systems to estimate number of occurrences in a given time period
  - Use descriptive adjectives or a simple rating system
  - The Delphi approach

Step 3: Estimate Likelihood of Exploitation

- Delphi approach is a subjective probability technique [Rand 67]
  - Designed to deal with public policy decisions
  - Assumes experts can make informed estimates based on their experience
    - the method brings a group of experts to consensus

Step 3: Estimate Likelihood of Exploitation

- The Delphi approach:
  - Provide each of several experts with information describing the situation surrounding the event under consideration
    - For example, the experts may be told about the software and hardware architecture, conditions of use, and expertise of users.
  - Each expert individually estimates the likelihood of the event
    - The estimates are collected, reproduced, and distributed to all experts.
  - The individual estimates are listed anonymously
    - the experts are usually given some statistical information, such as mean or median.

Step 3: Estimate Likelihood of Exploitation

- The Delphi approach (cont.)
  - The experts are then asked whether they wish to modify their individual estimates
    - in light of values their colleagues have supplied.
  - If the revised values are reasonably consistent, the process ends with the group's reaching consensus.
  - If the values are inconsistent, additional rounds of revision may occur until consensus is reached.

Quantitative vs. Qualitative Estimation

	Pros	Cons
Quantitative	• Assessment and results based on independently objective processes and metrics. Meaningful statistical analysis is supported • Value of information assets and expected loss expressed in monetary terms. Supporting rationale easily understood • Provides credible basis for cost/benefit assessment of risk mitigation. Supports information security budget decision-making	• Calculations are complex. Management may mistrust the results of calculations and hence analysis • Must gather substantial information about the target IT environment • No standard independently developed and maintained threat population and frequency knowledge base. Users must rely on the credibility of the in-house or external threat likelihood assessment
Qualitative	• Simple calculations, readily understood and executed • Not necessary to quantify threat frequency and impact data • Not necessary to estimate cost of recommended risk mitigation measures and calculate cost/benefit • A general indication of significant areas of risk that should be addressed is provided	• Results are subjective. Use of independently objective metrics is eschewed • No effort to develop an objective monetary basis for the value of targeted information assets • Provides no measurable basis for cost/benefit analysis of risk mitigation. Difficult to compare risk to control cost • Not possible to track risk management performance objectively when all measures are subjective

Step 4: Compute Expected Loss

- In addition to the obvious costs, such as the cost to replace a hardware asset, there are hidden costs:
  - Cost of restoring the system to a previous state
  - Cost of downtime
  - Legal fees
  - Loss of reputation and confidence
  - Loss of confidentiality

Step 4: Compute Expected Loss

- Some hidden costs may be impossible to accurately evaluate, but considering them will nonetheless aid in risk management

Step 5: Survey and Select New Controls

- Once you understand your assets, vulnerabilities, estimated likelihood of exploitation, and cost of exploitation, you have enough information to select controls

Step 5: Survey and Select New Controls

- Each vulnerability may have one or more controls associated with it
  - each control may work for many assets and multiple vulnerabilities
- One approach is to use graph theory
  - to select a minimal set of controls to address all vulnerabilities

Step 6: Project Costs and Savings

- This step is meant to determine whether the costs of implementing controls outweigh the expected benefits
- The effective cost of a given control is the actual cost of the control minus the expected loss the control is expected to prevent
  - including purchase price, installation and deployment costs, and training costs

Step 6: Project Costs and Savings

- The cost may be positive if the product is very expensive or introduces new risks to the system
  - may be negative if the expected reduction in risk is greater than the cost of the control

Access Control Software Cost Example

Item	Amount
Risks: disclosure of company confidential data, computation based on incorrect data	
Cost to reconstruct correct data: $1,000,000 @ 10% likelihood per year	$100,000
Effectiveness of access control software: 60%	– 60,000
Cost of access control software	+25,000
Expected annual costs due to loss and controls (100,000 – 60,000 + 25,000)	$65,000
Savings (100,000 – 65,000)	$35,000

Arguments for Risk Analysis

- Improve awareness
- Relate security mission to management objectives
- Identify assets, vulnerabilities, and controls
- Improve basis for decisions
- Justify expenditures for security

Arguments for Risk Analysis

- Improve awareness
  - Issues of security can raise the general level of interest and concern among developers and user
    - Especially when the user population has little expertise in computing
    - The risk analysis can educate users about the role security plays in protecting functions and data that are essential to user operations and products.
- Relate security mission to management objectives
  - Security is often perceived as a financial drain for no gain
  - Management does not always see that security helps balance harm and control costs

Arguments for Risk Analysis

- Identify assets, vulnerabilities, and controls
  - Some organizations are unaware of their computing assets, their value to the organization, and the vulnerabilities associated with those assets
  - A systematic analysis produces a comprehensive list of assets, valuations, and risks
- Improve basis for decisions
  - A security manager can present an argument such as "I think we need a firewall here" or "I think we should use token-based authentication instead of passwords."
  - Risk analysis augments the manager's judgment as a basis for the decision

Arguments for Risk Analysis

- Justify expenditures for security
  - Some security mechanisms appear to be very expensive and without obvious benefit.
  - A risk analysis can help identify instances where it is worth the expense to implement a major security mechanism.
  - Managers can show the much larger risks of *not* spending for security

Arguments Against Risk Analysis

- False sense of precision and confidence
- Hard to perform
- Immutability
- Lack of accuracy

Arguments Against Risk Analysis

- False sense of precision and confidence
  - The heart of risk analysis is the use of empirical data to generate estimates of risk impact, risk probability, and risk exposure.
  - The danger is that these numbers will give us a false sense of precision, thereby giving rise to an undeserved confidence in the numbers.

Arguments Against Risk Analysis

- False sense of confidence (cont.):
  - In many cases the numbers themselves are much less important than their relative sizes
    - E.g., whether an expected loss is $100,000 or $150,000 is relatively unimportant.
    - It is much more significant that the expected loss is far above the $10,000 or $20,000 budget allocated
      - for implementing a particular control
    - Moreover, anytime a risk analysis generates a large potential loss, the system deserves further scrutiny
      - to see if the root cause of the risk can be addressed.

Arguments Against Risk Analysis

- Hard to perform:
  - Enumerating assets, vulnerabilities, and controls requires creative thinking.
  - Assessing loss frequencies and impact can be difficult and subjective.
  - A large risk analysis must consider many factors.
    - Risk analysis can be restricted to certain assets or vulnerabilities, however.
-

Arguments Against Risk Analysis

- *Immutability:*
  - Many software project leaders view processes such as risk analysis as an irritating fact of life
    - A step to be taken in a hurry so that the developers can get on with the more interesting jobs
      - related to designing, building, and testing the system
  - Therefore, risk analyses, like contingency plans and five-year plans, have a tendency to be filed and promptly forgotten
    - But if an organization takes security seriously, it will view the risk analysis as a living document, updating it at least annually
      - or in conjunction with major system upgrades.

Arguments Against Risk Analysis

- *Lack of accuracy:*
  - Risk analysis is not always accurate, for many reasons:
    - We may not be able to calculate the risk probability with any accuracy, especially when we have no past history of similar situations
    - Even if we know the likelihood, we cannot always estimate the risk impact very well.
      - The risk management literature is replete with papers about describing the scenario, showing that presenting the same situation in two different ways to two equivalent groups of people can yield two radically different estimates of impact.
    - .

Arguments Against Risk Analysis

- *Lack of accuracy:*
  - Risk analysis is not always accurate, for many reasons (cont.):
    - We may not be able to anticipate all the possible risks.
      - For example, bridge builders did not know about the risks introduced by torque from high winds until the Tacoma Narrows Bridge twisted in the wind and collapsed.
        - After studying the colossal failure of this bridge and discovering the cause, engineers made mandatory the inclusion of torque in their simulation parameters.
      - Similarly, we may not know enough about software, security, or the context in which the system is to be used
        - there may be gaps in our risk analysis that cause it to be inaccurate.

Natural Disasters

- Examples:
  - Flood
  - Fire
  - Earthquake

Natural Disasters

- Mitigations:
  - Develop contingency plans so that people know how to react in emergencies and business can continue
  - Insure physical assets—computers, buildings, devices, supplies—against harm
  - Preserve sensitive data by maintaining copies in physically separated locations
  - Prevent power loss using uninterruptable power supplies and surge suppressors

Interception of Sensitive Information

- Mitigations:
  - Shred paper copies of sensitive information
  - Overwrite magnetic data several times using software designed for that purpose
  - Degauss magnetic media
  - Protect against RF emanation by trapping signals or adding spurious ones

Contingency Planning

- Backups
  - Offsite backup
  - Cloud backup
- Failover
  - Cold site
  - Hot site

Summary

- A security plan is both an official record of current security practices and a blueprint for orderly change to improve those practices
- Business contingency and incident response planning help establish an orderly, carefully considered response to emergencies
  - and other security incidents

Summary

- Risk analysis is a complex and imperfect process
  - forces an organization to carefully consider important assets, vulnerabilities, risks, and control options
- Prepare for disasters by contingency planning, insuring assets, backing up data, and deploying failover sites

Questions?

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.