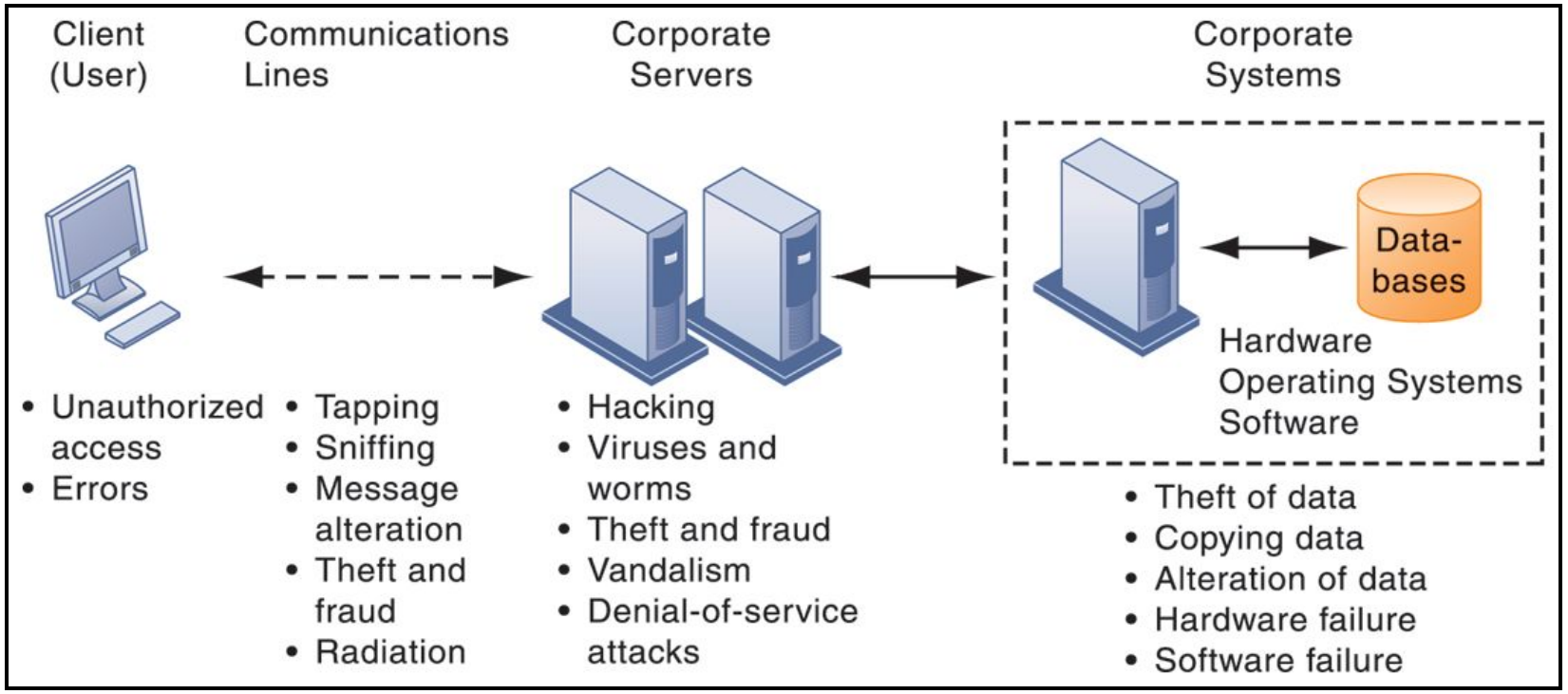
Chapter Six

Information systems Security and Control

Securing Information Systems

- **Why are systems vulnerable?**
  - Accessibility of networks
  - Hardware problems (breakdowns, configuration errors, damage from improper use or crime)
  - Software problems (programming errors, installation errors, unauthorized changes)
  - Disasters
  - Use of networks/computers outside of firm's control
  - Loss and theft of portable devices

Cont.


Client (User)
Communications Lines
Corporate Servers
Corporate Systems
Data-bases
Hardware
Operating Systems
Software
• Unauthorized access
• Errors
• Tapping
• Sniffing
• Message alteration
• Theft and fraud
• Radiation
• Hacking
• Viruses and worms
• Theft and fraud
• Vandalism
• Denial-of-service attacks
• Theft of data
• Copying data
• Alteration of data
• Hardware failure
• Software failure

Introduction

- We will consider administrative and physical aspects for security control with related to four areas:
  - Planning. What advance preparation and study lets us know that our implementation meets our security needs for today and tomorrow?
  - Risk analysis. How do we weigh the benefits of controls against their costs, and how do we justify any controls?
  - Policy. How do we establish a framework to see that our computer security needs continue to be met?
  - Physical control. What aspects of the computing environment have an impact on security?

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.
- **Contents of a Security Plan:** Every security plan must address seven issues.
  - **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
  - **accountability** , describing who is responsible for each security activity
  - **timetable ,** identifying when different security functions are to be done
  - **continuing attention** , specifying a structure for periodically updating the security plan

Security Planning Team Members

- A security planning team should represent each of the following groups.
  - computer hardware group
  - system administrators
  - systems programmers
  - applications programmers
  - data entry personnel
  - physical security personnel
  - representative users
  - Steering Committee Members

Assuring Commitment to a Security Plan

- After the plan is written, it must be accepted and its recommendations carried out.
- Commitment to the plan means that security functions will be implemented and security activities carried out.
- 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 for the way they will use the system and perform their business activities.
  - Management must be committed to using and enforcing the security aspects of the system.

Business Continuity Plans

- A **business continuity plan** documents how a business will continue to function during a computer security incident.
- A business continuity plan deals with 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
- The steps in business continuity planning are these:
  - Assess the business impact of a crisis.
  - Develop a strategy to control impact.
  - Develop and implement a plan for the strategy

Assess Business Impact

- Begin by asking two key questions:
  - What are the ***essential assets****? What are the things that will* prevent the business from doing business?
  - What could ***disrupt use of these assets****? The vulnerability is* more important than the threat agent.

Develop Strategy

- The continuity strategy investigates how the key assets can be safeguarded.
  - In some cases, a backup copy of data or redundant hardware or an alternative manual process is good enough.
  - Sometimes, the most reasonable answer is reduced capacity.
- The result of a strategy analysis is a selection of the best actions, organized by circumstances.
- The strategy can then be used as the basis for your business continuity plan

Develop Plan

- The business continuity plan specifies several important things:
  - who is in charge when an incident occurs
  - what to do
  - who does it
- The plan justifies making advance arrangements, such as acquiring redundant equipment, arranging for data backups, and stockpiling supplies, before the catastrophe.
- The plan also justifies advance training so that people know how they should react.

Incident Response Plans

- An **incident response plan** tells the staff how to deal with a security incident.
- In contrast to the business continuity plan, the goal of incident response is handling the current security incident, without 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*

Risk Analysis

- Good, effective security planning includes a careful risk analysis .
  - ✔ A risk is a potential problem that the system or its users may experience.
- distinguish a risk from other project events by looking for three things:
  - A loss associated with an event: This loss is called the **risk impact**.
  - The likelihood that the event will occur
    - ✔ The probability of occurrence associated with each risk is measured from 0(impossible) to 1 (certain).
  - The degree to which we can change the outcome
    - ✔ Risk control involves a set of actions to reduce or eliminate the risk.

Cont.

- three strategies for dealing with risk:
  1. *avoiding* the risk, by changing requirements for security or other system characteristics
  2. *transferring* 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
  3. *assuming* the risk, by accepting it, controlling it with available resources, and preparing to deal with the loss if it occurs
- Thus, costs are associated not only with the risk's potential impact but also with reducing it.
- **Risk leverage** is the difference in risk exposure divided by the cost of reducing the risk. In other words, risk leverage is

$$\frac{\text{(risk exposure before reduction)} - \text{(risk exposure after reduction)}}{\text{(cost of risk reduction)}}$$

Cont.

- 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.

Identify Assets

- Decide what we need to protect
- Thus, identify the assets of the computing system
- E.g.,
  - ***hardware**: processors, boards, communications media, …*
  - ***software**: source programs, object programs, OS, ….*
  - ***data**: data used during execution, stored data on various media, …*
  - ***people**: skills needed to run the computing system or specific programs*
  - ***documentation**: on programs, hardware, systems, ….*
  - ***supplies**: paper, forms, laser cartridges, magnetic media, …*

Determine Vulnerabilities

- Want to predict what damage might occur to the assets and from what sources
- Can use a matrix

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

Estimate Likelihood of Exploitation

- Determine how often each exposure is likely to be exploited.
- Several approaches to computing the probability that an event will occur: classical, frequency, and subjective.

Frequency	Rating
More than once a day	10
Once a day	9
Once every three days	8
Once a week	7
Once in two weeks	6
Once a month	5
Once every four months	4
Once a year	3
Once every three years	2
Less than once in three years	1

Compute Expected Loss

- Determine the likely loss if the exploitation does indeed occur.

Organizational Security Policies

- A security policy is a high-level management document to inform all users of the goals of and constraints on using a system
- A security policy must answer three questions: who can access which resources in what manner ?
- It should be a visible representation of priorities of the entire organization, definitively stating underlying assumptions that drive security activities.

Purpose

- Security policies are used for several purposes, including the following:
  - recognizing sensitive information assets
  - clarifying security responsibilities
  - promoting awareness for existing employees
  - guiding new employees

Characteristics of a Good Security Policy

- **Coverage** -A security policy must be comprehensive:
  - It must either apply to or explicitly exclude all possible situations
- **Durability** -A security policy must grow and adapt well.
  - In large measure, it will survive the system's growth and expansion without change
- **Realism** -The policy must be realistic .
  - That is, it must be possible to implement the stated security requirements with existing technology
- **Usefulness** -An obscure or incomplete security policy will not be implemented properly, if at all.
  - The policy must be written in language that can be read, understood, and followed by anyone who must implement it or is affected by it

Physical Security

- **Physical security** is the term used to describe protection needed outside the computer system.
- Natural Disasters
  - Flood
  - Fire
  - Other Natural Disasters
- Power Loss
  - Uninterruptible Power Supply
- Human Vandals
  - Unauthorized Access and Use
  - Theft
  - Preventing Access
  - Preventing Portability
  - Detecting Theft

Technologies and Tools for Protecting Information Resources

- Identity management software
- Authentication
- Firewalls
- Intrusion detection systems
- Antivirus and antispyware software
- Unified threat management (UTM) systems
- WAP2 specification for wireless networks
- Encryption

Thank you !!!!