Week 9
Control, audit and security

Learning Objectives

• Recognize the difficulties in managing information resources.
• Recognize information systems' vulnerability and the possible damage from malfunctions.
• Describe the major methods of defending information systems.

Learning Objectives (cont.)

• Describe the security issues of the Web and electronic commerce.
• Distinguish between security auditing and disaster recovery planning and understand the economics of security.

Case: Cyber Crime

• On Feb. 6, 2000 - the biggest EC sites were hit by cyber crime. Yahoo!, eBay, Amazon.com, E*Trade
• The attacker(s) used a method called denial of service (DOS).
  – By hammering a Web site’s equipment with too many requests for information, an attacker can effectively clog a system.
• The total damage worldwide was estimated at $5-10 billion (U.S.).
  – The alleged attacker, from the Philippines, was not prosecuted because he did not break any law in the Philippines.

Lessons Learned from the Case

• Information resources that include computers, networks, programs, and data are vulnerable to unforeseen attacks.
• Many countries do not have sufficient laws to deal with computer criminals.
• Protection of networked systems can be a complex issue.

Lessons Learned from the Case

• Attackers can zero on a single company, or can attack many companies, without discrimination.
• Attackers use different attack methods.
• Although variations of the attack methods are known, the defence against them is difficult and/or expensive.
Information Resources Management

- IRM encompasses all activities related to the planning, organizing, acquiring, maintaining, securing, and controlling of IT resources.
- The management of information resources is divided among the information services department (ISD) and the end-users.

End-User Computing

- Establish policies and procedures to control end-user computing so that corporate risks are minimized.
- Create incentives to encourage certain end-user practices that reduce organizational risks.
- Offer support. Develop services to aid end-users in their computing activities.

Steering Committees

The corporate steering committee is a group of managers and staff representing various organizational units. The committee’s major tasks are:
- Direction setting
- Staffing
- Rationing
- Communication
- Structuring
- Evaluating

Key Terminology

- Decryption
- Encryption
- Backup
- Exposure
- Integrity (of data)
- Risk
- Threats (or hazards)
- Vulnerability

Security Threats

Cyber Crime

- Crimes can be performed by outsiders who penetrate a computer system (hackers) or by insiders who are authorized to use the computer system but are misusing their authorization.
- Two basic methods of attack are used in deliberate attacks on computer systems:
  - data tampering
  - programming fraud, e.g. Viruses
Defending Information Systems

Defending information systems is not a simple or inexpensive task for the following reasons:

- Hundreds of potential threats exist.
- Computing resources may be situated in many locations.
- Many individuals control information assets.
- Rapid technological changes make some controls obsolete as soon as they are installed.
- Many computer crimes are undetected for a long period of time.
- People tend to violate security procedures because they are inconvenient.

Defense Strategies

- The following are the major objectives of defense strategies:
  - Prevention & deterrence
  - Detection
  - Limitation
  - Recovery
  - Correction

Types of Controls

- General Controls
  - Physical controls
  - Access controls
  - Biometric controls
  - Data security controls
  - Communications (networks) controls
  - Administrative controls

- Application Controls
  - Input controls
  - Processing controls
  - Output controls

Security Measures

- An access control system guards against unauthorized dial-in attempts.
  - The use of preassigned personal identification number (PIN).
- Modems. It is quite easy for attackers to penetrate them and for employees to leak secret corporate information to external networks.
- Encryption is used extensively in EC for protecting payments and privacy.
- Troubleshooting packages such as cable tester can find almost any fault that can occur with LAN cabling.
- Payload security involves encryption or other manipulation of data being sent over networks.
- Commercial Products. Hundreds of commercial security products exist on the market.
- Intrusion Detecting. It is worthwhile to place an intrusion detecting device near the entrance point of the Internet to the intranet.
- A Firewall is commonly used as a barrier between the secure corporate intranet, or other internal networks, and the Internet.

IT Auditing

- In the information system environment, auditing can be viewed as an additional layer of controls or safeguards.
  - It involves a periodical examination and check of financial and accounting records and procedures.
- Two types of auditors (and audits):
  - Internal
    - An internal auditor is usually a corporate employee who is not a member of the ISD.
  - External
    - An external auditor is a corporate outsider.
Auditors attempt to answer questions such as:

1. Are there sufficient controls in the system?
2. Which areas are not covered by controls?
3. Which controls are not necessary?
4. Are the controls implemented properly?
5. Are the controls effective; do they check the output of the system?
6. Is there a clear separation of duties of employees?
7. Are there procedures to ensure compliance with the controls?
8. Are there procedures to ensure reporting and corrective actions in case of violations of controls?

A disaster recovery plan is essential to any security system.

- The purpose of a recovery plan is to keep the business running after a disaster occurs.
- Recovery planning is part of asset protection.
- Planning should focus first on recovery from a total loss of all capabilities.
- Proof of capability usually involves some kind of what-if analysis that shows that the recovery plan is current.
- All critical applications must be identified and their recovery procedures addressed in the plan.

In the event of a major disaster, it is often necessary to move a centralized computing facility to a far-away backup location.

- External hot-site vendors provide access to a fully configured backup data center.

The objective relating to reliability is to use fault tolerance to keep the information systems working, even if some parts fail.

Artificial Intelligence in Biometrics.

Expert systems, neural computing, voice recognition, and fuzzy logic can be used to enhance the capabilities of several biometric systems.

Smart Cards. Smart card technology can be used to protect PCs on LANs.

Fighting Hackers. Several new products are available for fighting hackers.
Control

What is controlled?
- assets
- physical access
- operational procedures
- financial transactions
- inventory related transactions
- personnel related transactions
- management procedures

Access controls
- to the computer centre equipment
- to the application software
- to offices
- to product warehouses
- control technologies

Operational controls
- rationale for operational (process) controls
- goals
- mechanisms
- a control framework

Control objectives
- operation of a business process achieves the goal set for it
- correct information is provided to a business process
- operation of the business process is available only to authorised personnel
- the business process only occurs in appropriate operational circumstances

Privacy — a security issue
- corporate information
- customer/client information
- liability and responsibility

References
- Chapter 16, Frenzel and Frenzel
- Turban, Leidner, McLean & Wetherbe Chapter 15