Managing Information Resources and IT Security

Management Information

- Code: 164292-02
- Course: Management Information
- Period: Autumn 2013
- Professor: Sync Sangwon Lee, Ph. D
- D. of Information & Electronic Commerce

00. Contents

01. IS Department

- IS Department
  - IT resources are very diversified; they include personnel assets, technology assets, and IT relationship assets.
  - The management of information resources is divided between the information services department (ISD) and the end users.
  - The division of responsibility depends on many factors.

01. IS Department

- IS Department
  - The reporting relationship of the ISD is important in that it reflects the focus of the department.
  - If the ISD reports to the accounting or finance areas, there is often a tendency to emphasize accounting or finance applications at the expense of those in the marketing, production, and logistics areas.
  - The name of the ISD is also important.
    - Data processing department. (DPD)
    - Management information systems (MIS) department
    - Information systems department (ISD)
  - Another important characteristic is the status of the ISD.

01. IS Department

- End-User Relationship
  - Since the ISD is a service organization that manages the IT infrastructure needed to carry on end-user IT applications.
  - It is extremely important to have a good relationship with the end users.
  - The development of end-user computing and outsourcing was motivated in part by the poor service that end users felt they received.
  - However, this is not an easy task since the ISD is basically a technical organization that may not understand the business and the users.
  - While the users, may not understand information technologies.

01. IS Department

- End-User Relationship
  - To improve collaboration, the ISD and end users may employ three common arrangements:
    - Steering committee
    - Service-level agreements (SLA)
    - Information center.

Service Level Agreement Checklist

No	Procedures	Status	Notes
1	Are you using an independent expert to develop SLAs?		
2	Have you scoped the area to be covered by SLAs?		
3	Does the SLA consider BTOPP implications?		
4	Have the outputs for those areas been defined?		
5	Do they tie back to the business objectives?		
6	What is being measured?		
7	Why is it being measured?		
8	How will measurement be done?		
9	Has the current performance level been agreed?		
10	Has the current performance environment been documented?		
11	What are the new measures?		
12	Are the costs of achieving the new measures commensurate with the benefits?		
13	What changes are required to the environment to achieve these measures?		
14	What changes may take place that will alter these proposed measures?		
15	What changes may take place in the environment		

http://www.hipaacompliances.com

01. IS Department

- ISD and Four Approaches
  - 1) Let them sink or swim. Don’t do anything; let the end user beware.
  - 2) Use the stick. Establish policies and procedures to control end-user computing so that corporate risks are minimized, and try to enforce them.
  - 3) Use the carrot. Create incentives to encourage certain end-user practices that reduce organizational risks.
  - 4) Offer support. Develop services to aid end users in their computing activity

01. IS Department

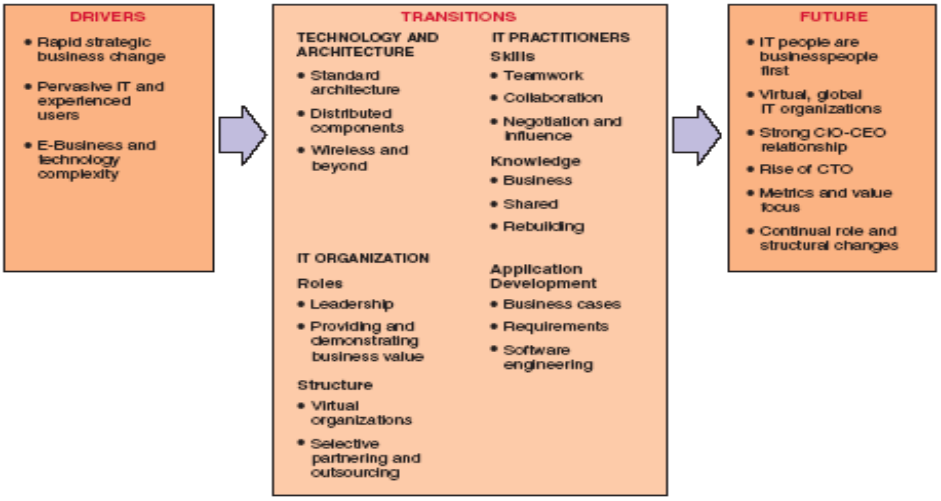
- Chief Information Officer (CIO)
  - Managing the ISD is similar to managing any other organizational unit.
  - The unique aspect of the ISD is that it operates as a service department in a rapidly changing environment, thus making the department’s projections and planning difficult.

01. IS Department

- Chief Information Officer (CIO)
  - The changing role of the ISD highlights the fact that the CIO is becoming an important member of the firm's top management team.
  - Realization of the need for IT-related disaster planning and the importance of IT to the firm's activities.
    - Aligning IT with the business strategy
    - Implementing state-of-the-art solutions
    - Providing information access
    - Being a business visionary who drives business strategy
    - Coordinating resources

01. IS Department

- Transition Environment



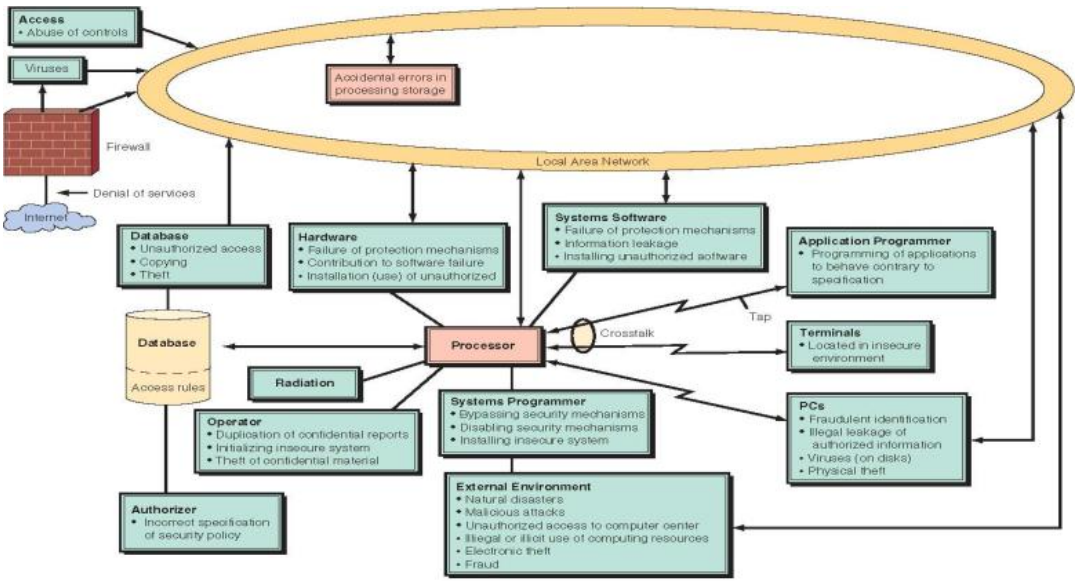
Information Technology for Management, Ed. 5, Efraim Turban et al., Wiley

02. IS Vulnerability

- IS Vulnerability
  - Information resources (physical resources, data, software, procedures, and other information resources) are scattered throughout the firm.
  - Information is transmitted to and from the firm's components. Therefore vulnerabilities exist at many points and at any time.

02. IS Vulnerability

- IS Vulnerability



Information Technology for Management, Ed. 5, Efraim Turban et al., Wiley

02. IS Vulnerability

- IT Security Terms

Backup	An extra copy of the data and/or programs, kept in a secured location(s).
Decryption	Transformation of scrambled code into readable data after transmission.
Encryption	Transformation of data into scrambled code prior to its transmission.
Exposure	The harm, loss, or damage that can result if something has gone wrong in an information system.
Fault tolerance	The ability of an information system to continue to operate (usually for a limited time and/or at a reduced level) when a failure occurs.
Information system controls	The procedures, devices, or software that attempt to ensure that the system performs as planned.
Integrity (of data)	A guarantee of the accuracy, completeness, and reliability of data. System integrity is provided by the integrity of its components and their integration.
Risk	The likelihood that a threat will materialize.
Threats (or hazards)	The various dangers to which a system may be exposed.
Vulnerability	Given that a threat exists, the susceptibility of the system to harm caused by the threat.

Information Technology for Management, Ed. 5, Efraim Turban et al., Wiley

02. IS Vulnerability

- System Vulnerability
  - A universal vulnerability is a state in a computing system which either:
    - Allows an attacker to execute commands as another user.
    - Allows an attacker to access data that is contrary to the access. restrictions for that data.
    - Allows an attacker to pose as another entity.
    - Allows an attacker to conduct a denial of service.

02. IS Vulnerability

- System Vulnerability
  - An exposure is a state in a computing system (or set of systems) which is not a universal vulnerability, but either:
    - Allows an attacker to conduct information gathering activities.
    - Allows an attacker to hide activities; includes a capability that behaves as expected, but can be easily compromised.
    - Is a primary point of entry that an attacker may attempt to use to gain access to the system or data.
    - Is considered a problem according to some reasonable security policy.

02. IS Vulnerability

- System Vulnerability
  - The vulnerability of information systems is increasing as we move to a world of networked and especially wireless computing.
  - Theoretically, there are hundreds of points in a corporate information system that can be subject to some threats.
  - These threats can be classified as
    - Unintentional
    - Intentional

02. IS Vulnerability

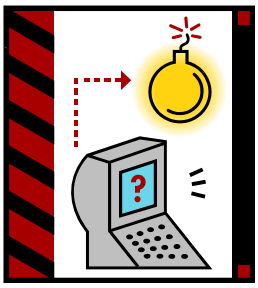
- System Vulnerability
  - Unintentional Threats
    - Human errors
    - Environmental hazards
    - Computer system failures

02. IS Vulnerability

- System Vulnerability
  - Intentional Threats
    - Theft of data
    - Inappropriate use of data
    - Theft of mainframe computer time
    - Theft of equipment and/or programs
    - Deliberate manipulation in handling
    - Entering/processing/transferring/programming data
    - Labor strikes
    - Riots
    - Sabotage
    - Malicious damage to computer resources
    - Destruction from viruses and similar attacks
    - Miscellaneous computer abuses
    - Internet fraud.
    - Terrorists' attack

03. Programming Attack

- Programming Attack
  - Programming attack is implemented through the modification of a computer program.



03. Programming Attack

- Methods of Programming Attack on Computer Systems

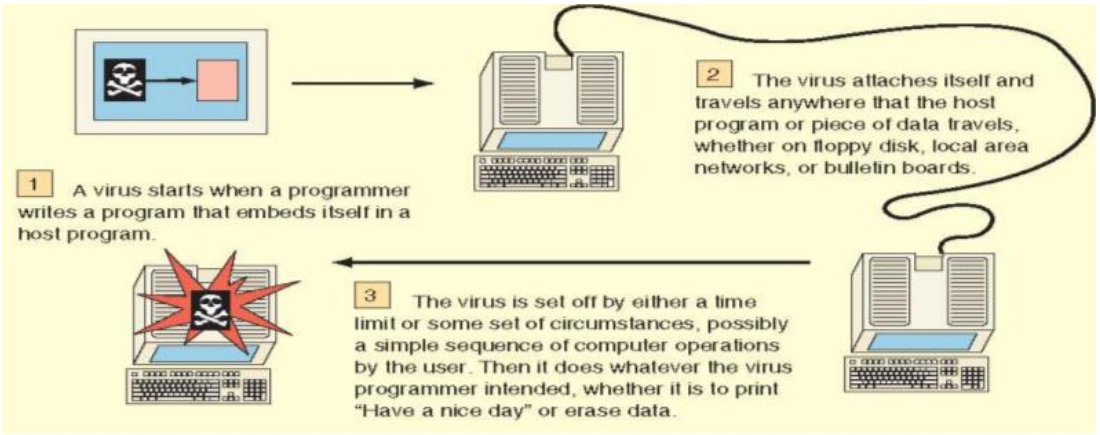
Method	Definition
Virus	Secret instructions inserted into programs (or data) that are innocently run during ordinary tasks. The secret instructions may destroy or alter data, as well as spread within or between computer systems.
Worm	A program that replicates itself and penetrates a valid computer system. It may spread within a network, penetrating all connected computers.
Trojan horse	An illegal program, contained within another program, that "sleeps" until some specific event occurs, then triggers the illegal program to be activated and cause damage.
Salami slicing	A program designed to siphon off small amounts of money from a number of larger transactions, so the quantity taken is not readily apparent.
Superzapping	A method of using a utility "zap" program that can bypass controls to modify programs or data.
Trap door	A technique that allows for breaking into a program code, making it possible to insert additional instructions.
Logic bomb	An instruction that triggers a delayed malicious act.
Denial of service	Too many requests for service, which crashes a Web site.
Sniffer	A program that searches for passwords or content in a packet of data as they pass through the Internet.
Spoofing	Faking an e-mail address or Web page to trick users to provide information or send money.
Password cracker	A password that tries to guess passwords (can be very successful).
War dialing	Programs that automatically dial thousands of telephone numbers in an attempt to identify one authorized to make a connection with a modem; then someone can use that connection to break into databases and systems.
Back doors	Invaders to a system create several entry points; even if you discover and close one, they can still get in through others.
Malicious applets	Small Java programs that misuse your computer resources, modify your file, send fake e-mail, etc.

03. Programming Attack

- Viruses
  - The most common attack method is the virus a program that attaches itself to (“infect”) other computer programs, without the owner of the program being aware of the infection.
  - It spreads, causing damage to that program and possibly to others.
  - When a virus is attached to a legitimate software program, the legitimate software is acting as a Trojan horse, a program that contains a hidden function.

03. Programming Attack

- Viruses



04. Protecting Information Resources

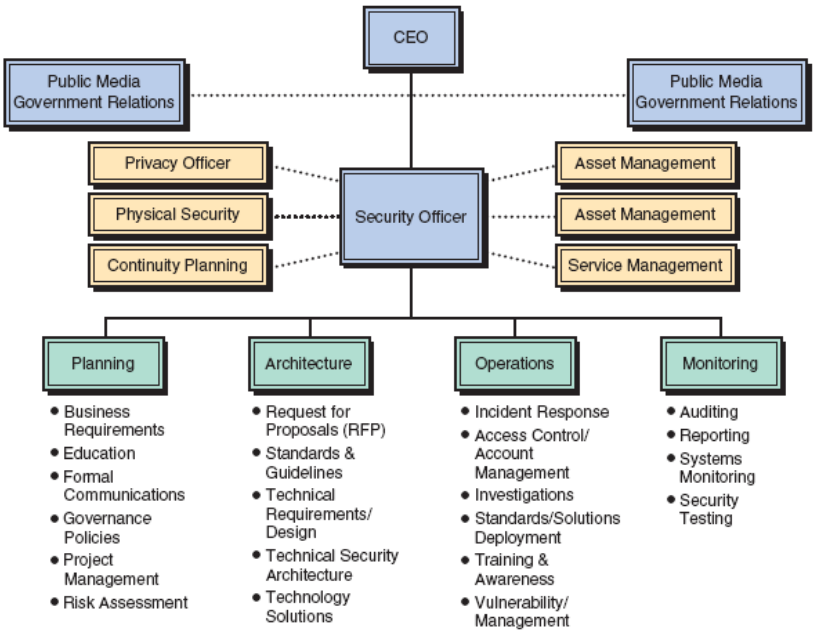
- Protecting Information Resources
  - Information security problems are increasing rapidly, causing damage to many organizations.
  - Protection is expensive and complex.
  - Therefore, companies must not only use controls to prevent and detect security problems, they must do so in an organized manner.

04. Protecting Information Resources

- Total Quality Management (TQM)
  - An approach similar to TQM (total quality management) would have the following characteristics:
    - Aligned: The program must be aligned with organizational goals.
    - Enterprise-wide: Everyone in the organization must be included.
    - Continuous: The program must be operational all the time.
    - Proactive: Use innovative, preventive, and protective measures.
    - Validated: The program must be tested to ensure it works.
    - Formal: It must include authority, responsibility & accountability.

05. Corporate Security Plan

- Corporate Security Plan - Protecting



05. Corporate Security Plan

- Difficulties in Protecting Information Resources

- Hundreds of potential threats exist, and they keep changing.
- Computing resources may be situated in many locations.
- Many individuals own or control information assets.
- Computer networks can be outside the organization and difficult to protect.
- Rapid technological changes make some controls obsolete as soon as they are installed. New threats (e.g., viruses) appear constantly.
- Many computer crimes are undetected for a long period of time, so it is difficult to learn from experience.
- People tend to violate security procedures because the procedures are inconvenient.
- Many computer criminals who are caught go unpunished, so there is no deterrent effect.
- The amount of computer knowledge necessary to commit computer crimes is usually minimal. As a matter of fact, one can learn hacking, for free, on the Internet.
- The cost of preventing some hazards can be very high. Therefore, most organizations simply cannot afford to protect against all possible hazards.
- It is difficult to conduct a cost-benefit justification for controls before an attack occurs since it is difficult to assess the value of a hypothetical attack.

05. Corporate Security Plan

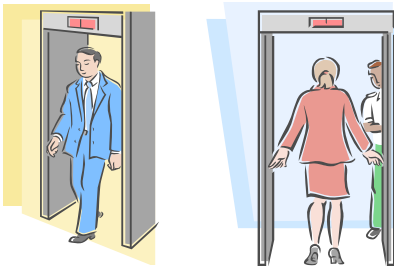
- Defense Strategy - Protecting
  - Knowing about potential threats to IS is necessary, but understanding ways to defend against these threats is equally critical.
  - Because of its importance to the entire enterprise, organizing an appropriate defense system is one of the major activities of the CIO.
  - It is accomplished by inserting controls (defense mechanisms) and developing awareness.

05. Corporate Security Plan

- Defense Strategy - Protecting
  - The major objectives of a defense strategy are:
    - Prevention and deterrence
    - Detection
    - Limitation of damage
    - Recovery
    - Correction
    - Awareness and compliance

05. Corporate Security Plan

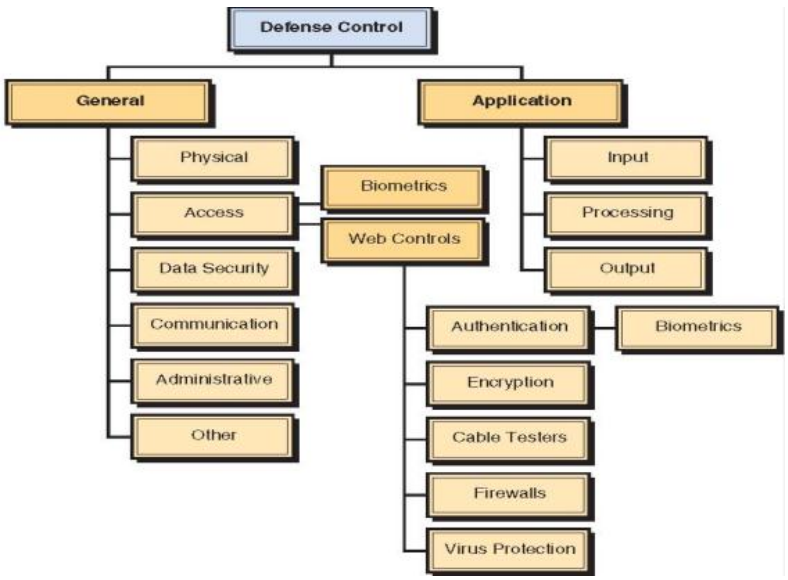
- Defense Strategy - Controls
  - Any defense strategy involves the use of several controls.
  - These controls are divided into two categories general controls that protect the system regardless of the specific application and application controls that safeguard specific applications.



05. Corporate Security Plan

- Defense Strategy - Controls

General

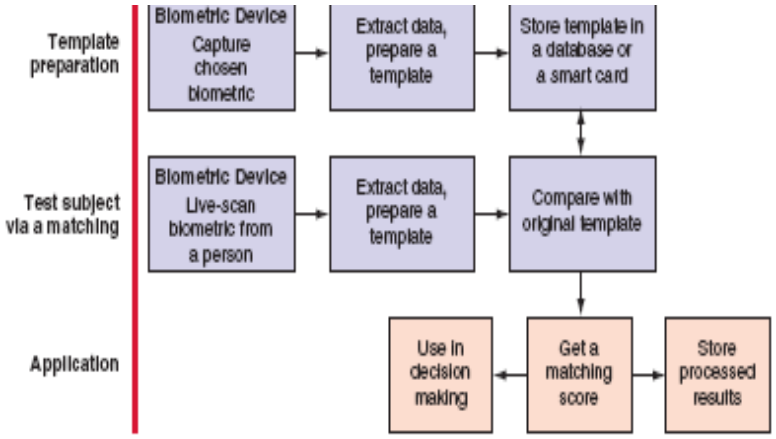


Application

Information Technology for Management, Ed. 5, Efraim Turban et al., Wiley

05. Corporate Security Plan

- Defense Strategy - Biometric
  - How a biometric system works



Information Technology for Management, Ed. 5, Efraim Turban et al., Wiley

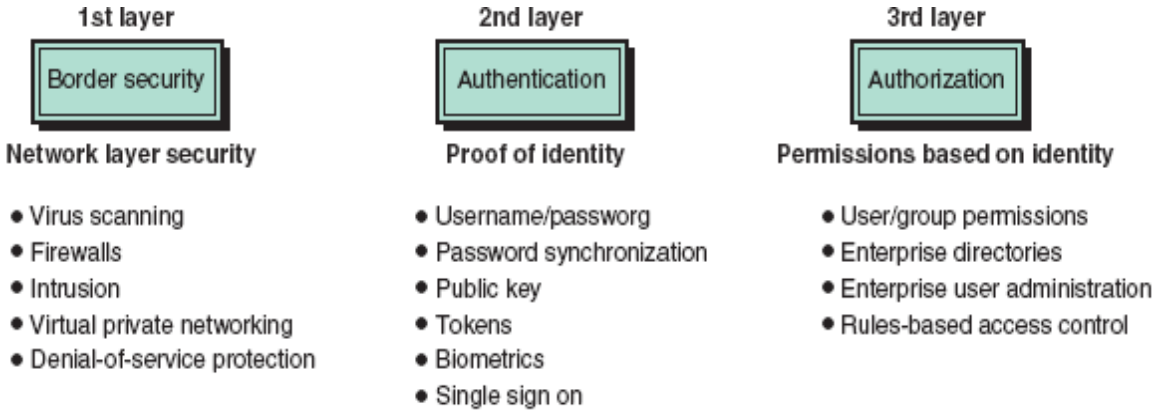
Management Information / 2013-2-WKU-MI-B15.pptx

05. Corporate Security Plan

- Defense Strategy - Internet Security
  - The major objective of border security is access control.
  - Then authentication or proof of identity and finally authorization which determine the action or activities a user is allowed to perform.

05. Corporate Security Plan

- Defense Strategy - Internet Security
  - Security layers



Information Technology for Management, Ed. 5, Efraim Turban et al., Wiley

06. Business Continuity

- Business Continuity
  - An important element in any security system is the business continuity plan, also known as the disaster recovery plan.
  - Such a plan outlines the process by which businesses should recover from a major disaster.

06. Business Continuity

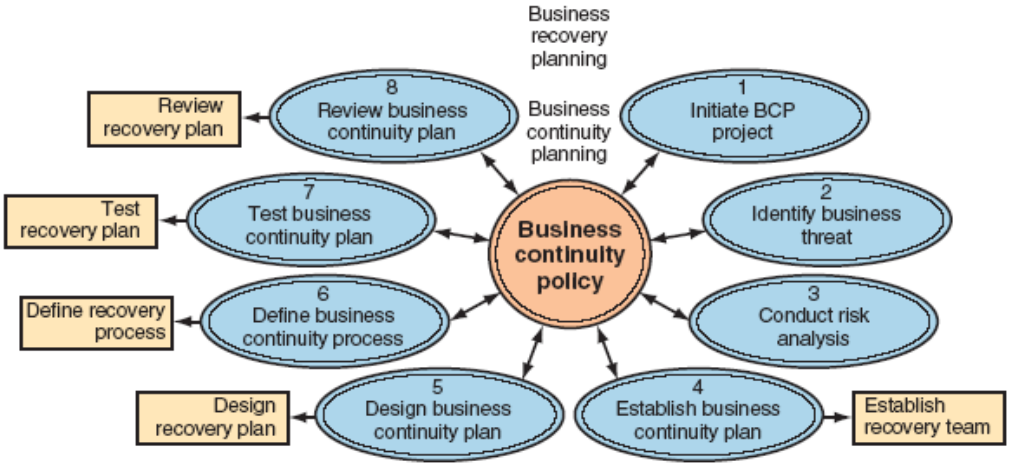
- Business Continuity
  - The purpose of a business continuity plan is to keep the business running after a disaster occurs.
  - Recovery planning is part of asset protection.
  - Planning should focus on recovery from a total loss of all capabilities.
  - Proof of capability usually involves some kind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

06. Business Continuity

- Business Continuity Plan
  - The plan should be kept in a safe place; copies should be given to all key managers; or it should be available on the Intranet and the plan should be audited periodically.
  - One of the most logical ways to deal with loss of data is to back it up.
  - A business continuity plan should include backup arrangements were all copies of important files are kept offsite.

06. Business Continuity

- Business Continuity Plan



Information Technology for Management, Ed. 5, Efraim Turban et al., Wiley

07. Auditing

- Auditing
  - Implementing controls in an organization can be very complicated and difficult to enforce.
  - These and other questions need to be answered by independent and unbiased observers.
    - Are controls installed as intended?
    - Are they effective?
    - Did any breach of security occur?
  - Such observers perform an auditing task.

07. Auditing

- Types of Auditors
  - Internal auditor
    - An internal auditor is usually a corporate employee who is not a member of the ISD.
  - External auditor
    - An external auditor is a corporate outsider.
    - This type of auditor reviews the findings of the internal audit.

07. Auditing

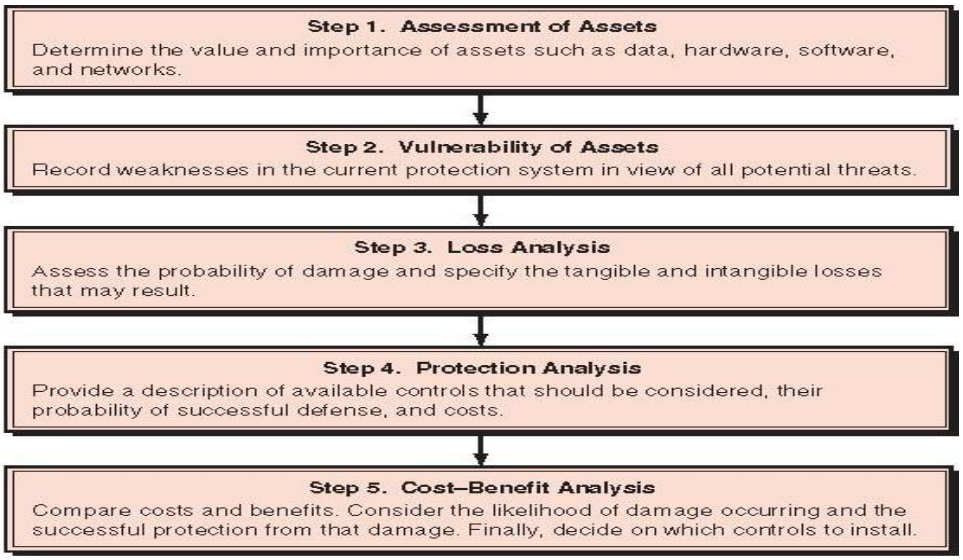
- Types of Audits
  - Operational audit
    - Determines whether the ISD is working properly.
  - Compliance audit
    - Determines whether controls have been implemented properly and are adequate.

08. Risk Management

- Risk Management
  - It is usually not economical to prepare protection against every possible threat.
  - Therefore, an IT security program must provide a process for assessing threats and deciding which ones to prepare for and which ones to ignore.

08. Risk Management

- Steps of Risk Management



Information Technology for Management, Ed. 5, Efraim Turban et al., Wiley

09. IT Security Trends

- IT Security Trends
  - Increasing the reliability of systems
  - Self-healing computers
  - Intelligent systems for early intrusion detection
  - Intelligent systems in auditing and fraud detection
  - Artificial intelligence in biometrics
  - Expert systems for diagnosis, prognosis, and disaster planning
  - Smart cards