Chapter 5: System Security

Overview

This chapter discusses system security; it may be one of the most important issues in this section. The increased use of networks (especially the Internet) has made systems more vulnerable to threats from inside and outside the organization. It is critical that all employees learn about keeping their systems safe and promote compliance throughout the organization.

Lecture Notes

A. Systems Personnel and Users

1. **Information Systems Personnel** are responsible for maintaining the hardware, software, data storage, and networks.
    a. Programmers are technical specialists who write and maintain software code.
    b. Systems analysts translate business requirements into IT problems.
    c. Database administrators are responsible for logical database design, security, and use of the database.
    d. Network engineers design and maintain the technology infrastructure.
    e. Web masters monitor and maintain Web pages; Web designers develop Web sites.

2. **System Users** (end users) include the business personnel that use the information system. *Emphasize the importance of protecting the environment.*
    a. Antivirus programs should be kept up-to-date and run often.
    b. Backup important documents regularly in case of emergency.
    c. Passwords should be applied to keep information secure.
    d. Permanently delete files that are unnecessary.
    e. Firewalls should be installed to protect the data.

3. **Systems Personnel and End-Users** must have a good working relationship because of the close tie between information systems and business operations.
    a. Technical and administrative support for users, training along with upgrades including:
        - Technology specialists
        - Training
        - Help desk
        - Technology support group
        - Technology updates

b. An information center supports users using technology.

c. Information policy sets up the guidelines for safe use of a computer system; it should be posted on the company Intranet.

d. Joint information systems/end-user teams are used in a team management system – collaborative efforts for planning and implementing all facets of the system.

e. A steering committee focuses on policies for the information system – priorities, budgeting, and security.

B. System Vulnerability

The vulnerability of a computer system has multiplied as technology advancements are made and the Internet is used so extensively. *This is one of the most important issues for students to understand as a computer user (at home or at the office). Emphasize its importance*.

1. **Threats to the Computer-Based Information System** come from internal and external sources.

a. Unintentional threats to the system include:

- Errors at any point in the information processing cycle; check for accuracy.
- Software defects and errors; check for patches regularly.
- Inaccurate or inconsistent data crates operational and financial problems.
- Environmental hazards – fire, floods, power outages, earthquakes, hurricanes and storms.

b. Intentional threats to the system include:

- Hackers access a computer system for mischief; crackers are malicious.
- Viruses are software programs that spread through a network disrupting operations.
- A Trojan horse is a destructive program that impersonates an innocent application.
- Spam is unsolicited junk mail.
- Data tampering whether it is intentional or not.

2. **Creating a Controlled Environment** is primarily the responsibility of the IT division, but everyone should be aware of the strategies for safety and security purposes.

a. General controls include:

- Avoid theft by locking all doors inside and out, using security personnel or cameras.
- Have a disaster recovery plan.
- Maintain and replace equipment on a rotating basis to avoid obsolescence.

- Restrict unauthorized users with passwords, access cards, or biometric controls.
- Be sure all software licenses are up-to-date and accurate.
- Implementation controls ensure that the system is properly managed.
- Testing programs identifies errors before they create problems for users; an acceptance test is used to evaluate the entire system.
- Conversion is the process of changing from one system to another.
  - Direct is all at once; risky and costly.
  - Parallel runs both at once; safe but costly.
  - Pilot tests in one area first.
  - Phased spreads out cost and training.
- Training and end-user support is important for an effective system.
- Fault-tolerant systems include a duplicate system as a backup during system failure.
- A disaster recovery plan should be in place to run a business during a system failure.
- Data security must be a part of the network and database systems; data backup and recovery.
- Data use controls include rules, standards, and disciplinary action; promote compliance.

b. Application controls are specific to each application. They include:
   - Input controls check for authorization, data editing, and error handling.
   - Processing controls check for accuracy in the data and completeness during the processing phase.
   - Output controls ensure that the end results are complete and properly distributed.

c. Network and internet security controls help deal with crackers and computer viruses.
   - Firewalls consist of software and hardware placed between the organization's internal network and an external network (the Internet).
   - Antivirus programs should be on all networks and computers to protect computers from viruses (both known and new); reduce vulnerability by keeping it current and training employees to be careful. *Review the guidelines presented in the text.*

d. E-commerce security is very important when data is being transmitted between buyers and sellers.
   - Encryption codes messages to restrict access; as many as 128 characters may be used to represent one character.

- A digital signature adds a code to a document to ID the sender and contents.
- A digital certificate uses a third party to verify the sender.
- A digital wallet is software that stores information for e-commerce.
- Security protocol (S-HTTP) is used to transfer information securely over the Internet.

C. System Quality Management: Troubleshooting

An information systems plan must support the business plan, so it is constantly changing along with the security methods.

1. **Systems Life Cycle** is important regardless of the size of the system; it requires interaction with personnel at all levels in the organization.
    a. Analysis is the problem-solving stage where causes and solutions are identified.
    b. Design is the blueprint or model of the system; the end user should have input into the design of the system.
    c. Development is the programming, testing, documenting, training, and converting to a new system.
    d. Operation and maintenance is continually assessing and making changes to the system; it is an ongoing process.
2. **Troubleshooting – Systems Analysis**
    a. Analyze current operations related to objectives and information flow.
    b. Identify existing problems and/or inefficiencies within the present system.
    c. Define alternatives for the user's new objectives.
    d. Evaluate the alternatives identified as they impact the organization (at all levels).
    e. Implementation and follow-up should continue.
3. **Troubleshooting – Systems Audits**
    a. External audit examines the input, process, output, internal audits, potential hazards.
    b. Internal audit should be done regularly by end-users, IT personnel, and corporate auditors for financial operations.

        Point out to students that Internal and external should include:

        - Output audits
        - Computer audits
        - Computer-assisted audits

    c. Data audits survey data files for accuracy and completeness; data cleansing should correct the problems that are found.

Additional Resources for Students

Recommended readings (no texts should be more than two years old):

- Fuller, Floyd and William Manning. *Computers and Information Processing*.
- Long, Larry and Nancy Long. *Introduction to Computers and Information Systems*. Prentice-Hall, Inc.
- Meyer, Marilyn and Roberta Baber. *Computers in Your Future*.
- Norton, Peter. *Introduction to Computers*.
- O'Leary, Timothy J. and Linda L. O'Leary. *Computing Essentials*. McGraw-Hill.
- Regan, Elizabeth A. and Bridget N. O'Connor. *Automating the Office – Office Systems and End-User Computing*. Macmillan City.
- Ricks, B., A. Swafford, and K. Gow. *Information and Image Management*. South-Western Publishing Co.
- Shelly, Gary and Thomas Cashman. *Learning to Use: Microcomputer Applications*. Boyd and Fraser Publishing Co.
- Tilton, R., J. Jackson, and S. Rigby. *The Electronic Office: Procedures and Administration*. South-Western Publishing Co.

Current issues of periodicals or business publications are also an excellent resource. Some of the following periodicals have an accompanying Web site.

Current Periodical	***Web Address***
Gregg Reference Manual	
IAAP Complete Office Handbook	http://www.iaap-hq.org/products/handbook.htm
Modern Office Technology	
Network Computing	http://www.networkcomputing.com/
Networking Management	
OfficePro	http://www.iaap-hq.org/officepro/toc.htm
PC Computing	