Computer Security

Chapter 1:

Organizational Policy

Learning Objectives:

1. After completing this section, you should be able to:
2. Identify requirements of the organizational security policies.
3. Recognize the three levels of security.
4. Recognize proper security safeguards.

Chapter 2:

Physical Security and Data Preservation

Learning Objectives:

1. After completing this section, you should be able to:
2. Recognize the different lines of defense for a computer system.
3. Identify environmental considerations as they apply to computer security.
4. Recognize the components of a maintenance log.
5. Identify computer access controls for software and data files.

Chapter 3:

Hardware Security

Learning Objectives:

After completing this section, you should be able to:

1. Identify some of the most common hardware problems.
2. Identify how data integrity may be threatened.
3. Recognize some hardware security devices used to protect the computer system.

Chapter 4:

Software Security

Learning Objectives:

After completing this section, you should be able to:

1. Identify top security related products in use.
2. Recognize different types of viruses and security threats.
3. Recognize the uses of firewall security systems.

Chapter 5:

Personnel Security

Learning Objectives:

After completing this section, you should be able to:

1. Identify prerequisites for sensitive personnel positions.
2. Recognize the value of an employee performance evaluation system and components of a training system.
3. Identify security issues posed by terminated employees.

Chapter 6:

Network Security

Learning Objectives:

After completing this section, you should be able to:

1. Recognize network tools used to implement security plans.
2. Identify the tools and techniques used by saboteurs.

Chapter 7:

Security Policy

Learning Objectives:

After completing this section, you should be able to:

1. Identify questions that policy makers should answer when designing a security system.
2. Recognize activities conducted as part of the risk analysis and management.
3. Recognize human factor threats for security.

Chapter 8:

Contingency Planning

Learning Objectives:

After completing this section, you should be able to:

1. Recognize the types of disruptions in computer processing.
2. Recognize components of a contingency plan.
3. Identify fire safety preventive plans.

Chapter 9:

Auditing and Legal Issues

Learning Objectives:

After completing this section, you should be able to:

1. Identify the scope of internal and external security auditing.
2. Recognize the audit trail to identify unusual activities.
3. Recognize control techniques.
4. Identify EDI security risks.

Chapter 10:

Computer Crime, Cyberfraud, and Recent Trends

Learning Objectives:

After completing this section, you should be able to:

1. Recognize penalties of the US Computer Fraud and Abuse Act.
2. Identify major issues regarding computer crimes and privacy issues.
3. Identify new certificate programs in computer security.