Computer Security

Course Description

The course is intended primarily to help business executives and information systems/computer professionals protect the computer and the data from a wide variety of threats. Security concerns have heightened in the recent years. Weak computer security and lack of internal controls increases an organization's vulnerability. The major steps in understanding and managing computer security are discussed in this course. The course helps business executives identify resources in their organizations that need to be protected.

Completion Deadline & Exam: This course, including the examination, must be completed within one year of the date of purchase. In addition, unless otherwise indicated, no correct or incorrect feedback for any exam question will be provided.

Course Level: Overview. This program is appropriate for professionals at all organizational levels.
CPE Credits: 9 (CPA)
Category: Computer Science
Prerequisite: None
Advanced Preparation: None

Course Learning Objectives

Chapter 1: Organizational Policy

After studying this chapter you will be able to:

1. Identify requirements of the organizational security policies.
2. Recognize the three levels of security.
3. Recognize proper security safeguards.

Chapter 2: Physical Security and Data Preservation

After studying this chapter you will be able to:

1. Recognize the different lines of defense for a computer system.

2. Identify environmental considerations as they apply to computer security.
3. Identify computer access controls for software and data files.

Chapter 3: Hardware Security

After studying this chapter you will 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

After studying this chapter you will 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

After studying this chapter you will be able to:

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

Chapter 6: Network Security

After studying this chapter you will 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

After studying this chapter you will 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

After studying this chapter you will 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

After studying this chapter you will 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

After studying this chapter you will 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.