COMPUTER SECURITY:
CRIME AND FRAUD PROTECTION

Delta Publishing Company

WHAT THIS COURSE WILL DO FOR YOU

COMPUTER SECURITY: PREVENTING COMPUTER CRIMES is written primarily to help business executives and information systems/computer professionals protect the computer and the data from a wide variety of threats. Computers are an integral part of everyday operations. Organizations are dependent upon their computer systems. A failure of the computer system is likely to have a critical impact on the organization. Potential vulnerabilities in a computer system could undermine operations and therefore, must be minimized or eliminated.

This course addresses a wide range of computer security issues. It is intended to provide practical and thorough guidance. The emphasis is on practical guidance rather than on theory. It helps managers improve computer security in their organizations.

Security concerns have heightened in the recent years. News events about computer related data errors, thefts, burglaries, fires, and sabotage dominate. The nature of the computing environment has changed significantly. The increased use of networked computers, including the Internet, Intranet, and Extranet, has had a profound effect on computer security. The greatest advantage of remote access via networks is convenience. This convenience makes the system more vulnerable to loss. As the number of points from which the computer can be accessed increases, so does the threat of attack. More caution is clearly needed to counter such threats. Weak computer security and lack of internal controls increases an organization's vulnerability.

The major steps in managing computer security are discussed in this course. We help business executives identify resources in their organizations that need to be protected. Sometime, the organization may not even consider the information to be "valuable" to anyone else and may not be willing to take security precautions. This is a serious mistake. Frequently, hackers are interested in obtaining access to private or confidential information. Hackers often steal or destroy data or information simply because it is there! Other hackers may delete or destroy files in an attempt to cover their illegal activity. The course highlights the need for a comprehensive security plan in an organization and explains why a casual attitude towards computer security is never justified.

The costs and benefits of various security safeguards are also discussed. The cost of a security safeguards includes not only the direct cost of the safeguards, such as equipment and installation costs, but also indirect costs such as employee morale and productivity. It is important to recognize that increasing security typically results in reduced convenience. For example, employees may resent the inconvenience that results from implementing security safeguards. Too much security can be just as detrimental as too little security; a balance must be maintained.

Special emphasis is given to contingency planning. Assuming that security is violated, how do you recover? What are the data backup policies? What are the legal consequences? What will be the financial impact? A risk analysis should be performed in planning computer security policies and financial support.

Computer security risks fall into one of three major categories: destruction, modification, and disclosure. Each of these may be further classified into intentional, unintentional and environmental attacks. The threat comes from computer criminals and disgruntled employees who intend to defraud, sabotage, and "hack". It also comes from computer users who are careless or negligent. Lastly, the threat comes from the environment; an organization must protect itself from disasters such as fire, flood, and earthquakes. An effective security plan must consider all three types of threats: intentional attacks, unintentional attacks, and environmental attacks.

Insurance is also discussed in the course. What is the company's degree of risk exposure? Insurance policies should be taken out to cover such risks as theft, fraud, intentional destruction, and forgery. Business interruption insurance covers lost profits during downtime.

This course addresses the security concerns of business managers. This course is designed as a practical, “how to” guide. We provide extensive examples to illustrate practical applications. The tools and techniques in this course can be adopted outright or modified to suit individual needs. Checklists, charts, graphs, diagrams, report forms, schedules, tables, exhibits, illustrations, and step-by-step instructions enhance the course’s practical use. Answers to commonly used questions are also given.

TABLE OF CONTENTS