CERIAS

LEARNING PRODUCTS

INFORMATION SECURITY MANAGEMENT SERIES

Your organization has many assets such as personnel, equipment, facilities, trade secrets, customer databases, engineering specifications, and marketing strategies. In today's knowledge economy, information is the most valuable asset, a resource you must protect. Thirty years ago there were no networks and computing was done on a mainframe. Five years ago commercial use of the Internet was allowed and the first macro virus was introduced. Today there are millions of systems in existence and more than 500 million users with access to networked systems on all seven continents. Advances in technology will turn the Internet into the "Evernet", where high-speed networking, truly mobile computing, and numerous embedded systems are deployed to billions of users worldwide. There is no better time to rethink how you manage information security than now.

This series is intended for managers and administrators concerned with intellectual property, corporate assets, infrastructure, and information assurance. This series will provide you with a current look at the information assurance landscape including intellectual property crime, threats to your information assets, vulnerabilities in information systems, and countermeasures to strengthen information assurance and security in your organization. This series consists of 4 modules described below.

Module 1: Foundations of information Security

Description

Are your trade secrets protected? Is necessary data available to your suppliers and customers to ensure efficient business operations? Can you verify the authenticity of a file sent to you by a business partner? These issues must be addressed if businesses wish to engage in eCommerce applications to maximize business opportunities and efficiencies.

This video/case study module will provide you with an overview of the foundational principles (confidentiality, availability, integrity, authenticity, access control, non-repudiation, utility, and control) goals of a sound information assurance and security program. In order to understand the policies, procedures, guidelines, training, and technology that your organization needs to protect your information assets, you need to understand these fundamental principles. This module is a prerequisite to the other modules in this series.

Topics

Information security principles/goals

- What they are
- Why they are important
- How to use them as the foundation for your information security program

Format

Available on CD-ROM or VHS videotape [NTSC or PAL format]

Length
45 minutes

Module 2: Information Security Risk Analysis
Description
What are your information security risks? What information security threats and vulnerabilities is your organization facing? And what are the costs of mitigating those information security risks? This module provides you with a comprehensive overview of issues you should know about in order to conduct a meaningful Information Security Risk Analysis.

This video/case study module shows you how to use cost effective risk analysis techniques to identify and quantify the threats to your organization, the origin of the threats, necessary countermeasures to reducing or eliminating the threat, and associated costs.

Prerequisites
Module 1: Current Approaches To Information Security: An Overview

Topics
Information security threats
- Types of threats
- Motives for computer crime
- Levels of associated risk

Common computer vulnerabilities
- How they relate to exploits, attacks, and flaws
- Types of vulnerabilities
- Characteristics of vulnerabilities
- Quantifying vulnerabilities and associated risk

Countermeasures
- Establishing an Effective InfoSec Program using a three pronged approach

Policy
Personnel
Technology
- Associated risk mitigation

Format
Available on CD-ROM or VHS videotape [NTSC or PAL format]

Length
75 minutes

Module 3: Information Security Policy
Description
Many people perceive information security to be a technology problem, when in fact hardware and software solutions alone cannot secure your information assets. The cornerstone of an effective information security architecture is well-written policy. Join this module for a closer look at information security policy.

This video/case study module shows you how to develop effective policy the mitigates your information security risks. After completing this module, your organization should be better prepared to establish information security policy that protects your information resources and guides employee behavior.

Prerequisites
Module 2: Information Security Risk Analysis

Topics
Why Implement Security Policy
Key definitions
· *Policies*
· *Procedures*
· *Guidelines*
Policy elements and format
The policy development process

Format
Available on CD-ROM or VHS videotape [NTSC or PAL format]

Length
75 minutes

Module 4: Information Security Training and Awareness
Description
Employees are your best firewall…..or they should be anyway. This module will highlight how to conduct security awareness and training that impacts employee behavior and makes your employees one of the most effective countermeasure in your Information Security Program.

This video/case study module shows you why many information security training and awareness programs fail and attributes of successful information security awareness and training programs.

Prerequisites
Module 1: Current Approaches to Information Security
Topics
o Poor security practices common to computer users
o Goals for an awareness and training program
o Failed security training and awareness initiatives: What Not To Do
o Attributes of Successful Information Security Training and Awareness Programs
o Selecting appropriate training and awareness for your organization

Format
Available on CD-ROM or VHS videotape [NTSC or PAL format]

Length
75 minutes