Certified Information Security Manager CISM, Part 4 of 4: Incident Management

Meet the expert: As a certified Microsoft Instructor, Ken has focused his career on various security aspects of computer and network technology since the early 1980s. He has offered a wide variety of IT training and high level consulting projects for Fortune 500 companies globally. Through the course of his extensive career, he has taught a full line of Microsoft, CompTIA, Cisco, and other high level IT Security curricula.

Prerequisites: This is part 4 in the series

Runtime: 04:09:35

Course description: This course talks about different parts of incident management, overview, organization, resources, ways of measuring it, procedures, current state of incident response capability, and how to develop an incident response plan. You will also learn how to coordinate with disaster recovery and responsibility and discovery plans and testing. It wraps up with a post incident activities investigation. This course is part of a series covering the ISACA Certified Information Security Manager (CISM).

Course outline:

Incident Management Overview
- Introduction
- Introduction to Incident Management
- Incident Management Overview
- Types of Events
- Types of Events Continued
- Goals of Incident Management
- BCP and DRP
- Goals of Incident Management Continued
- Summary

Incident Response Procedures
- Introduction
- Introduction to Incident Response Planning
- Importance of Incident Management
- Outcomes of Incident Management
- Incident Management
- Concepts
- Concepts Continued
- Incident Response
- Incident Management Systems
- Summary

Incident Management Organization
- Introduction
- Introduction to Incident Management Organization
- Incident Management Organization
- Responsibilities
- Responsibilities Continued
- Defining Security Incidents
- Senior Management Commitment
- Summary

Incident Management Resources
- Introduction
- Policies and Standards
- Incident Response Technology Concepts
- Personnel
- Roles and Responsibilities
- Skills
- Awareness and Education
- Audits
- Summary

Incident Management Objectives
- Introduction
- Defining Objectives
- The Desired State
- Strategic Alignment
- Other Concerns
- Summary

Incident Management Metrics and Indicators
- Introduction
- Defined Responsibilities
- Management Metrics and Monitoring
- Metrics and Minitoring Continued
- Other Things to Monitor
- Summary

Current State of Response Capability
- Introduction
- Threats
- Vulnerabilities
- Summary

Developing an Incident Response Plan
- Introduction
- Elements of an Incident Response Plan
- Gap Analysis
- BIA
- BIA Continued
- Escalation Process for Effective IM
- Identifying Security Incidents
- Incident Management and Response Teams
- Organizing, Training, and Equipping Response Staff
- Incident Notification Process
- Incident Management Plan Challenges
- Summary

Recovery Options
- Introduction
- Goals of Recovery Operations
- Mobile Sites
- Choosing a Site Selection
- Recovery Plan
- Incident Management Response Teams
- Network Service High Availability
- Storage High Availability
- Risk Transference
- BCP and DRP
- Summary

Testing Response and Recovery Plans
- Introduction
- Periodic Testing
- Testing IT Infrastructure
- Analyze Test Results
- Measuring the Test Results
- Summary

Executing the Plan
- Introduction
- Updating the Plan
- Intrusion Detection Policies
- Who to Notify About an Incident
- Recovery Operations
- Other Operations
- Forensic Investigation
- Hacker/Penetration Methodology
- Hacker/Penetration Methodology Continued
- Summary