Certified Information Systems Security Professional, Part 8 of 9: Incident Management

Meet the expert: Kevin is an international author, consultant and international >speaker. He is the official course development writer for ISC2 CISSP, ISACA CRISC

and mile2’s C)ISSO. Kevin has been educating IT professionals for over 30 years. He

also provides cyber security consulting and support services for organizations

around the world. Assisting them with setting up Information Security programs and

addressing areas ranging from in-depth risk analysis to policy creation and security

awareness.

Prerequisites: This series assumes a good understanding of enterprise networking and networking security. This is part 8 of a 9 part series.

Runtime: 01:45:08

Course description: This course covers incident management, types of laws and computer crimes and how to handle evidence, physical security and how to integrate with information security. This course is part of a series covering the ISC(2) Certified Information Systems Security Professional or CISSP.

Course outline:

Incident Management
- Introduction
- Seriousness of Computer Crimes
- Incidents
- Incident Management Priorities
- Incident Response Capability
- Incident Management Requires
- Preparing for a Crime Before It Happens
- Incident Response Phases
- Summary

Law
- Introduction
- Types of Law
- Foundational Concepts of Law
- Common Laws: Criminal
- Common Laws: Civil
- Common Laws: Administrative
- Intellectual Property Laws
- Software Licensing
- Summary

Computer Crime
- Introduction
- Historic Examples of Computer Crimes
- Who Perpetrates These Crimes
- Types of Motivation for Attacks
- Telephone Fraud
- Identification Protection and Prosecution
- Computer Crime and Its Barriers
- Countries Working Together
- Security Principles for International Use
- Determine if a Crime Has Been Committed
- When Should Law Enforcement Get Involved
- Citizen vs. Law Enforcement Investigation
- Investigation of Any Crime
- Summary

Evidence Handling
- Introduction
- Role of Evidence in a Trial
- General Rules for Evidence
- Evidence Requirements
- Evidence Collection Topics
- Chain of Custody and Evidence Processing
- Evidence Types
- Hearsay Rule Exception
- Privacy of Sensitive Data
- Privacy Issues: US Laws as Examples
- European Union Principles on Privacy
- Employee Privacy Issues
- Computer Forensics
- Trying to Trap the Bad Guy
- Companies Can Be Found Liable
- Sets of Ethics
- Ethics
- Summary
- Summary

Physical Security
- Introduction
- Physical Security
- Physical Security: Threats
- Different Types of Threats and Planning
- Facility Site Selection
- Devices Will Fail
- Controlling Access
- External Boundary Protection
- Lock Types
- Facility Access and Piggybacking
- Securing Mobile Devices
- Entrance Protection
- Perimeter Protection
- Perimeter Security
- Types of Physical IDS
- Sensors
- Facility Attributes
- Electrical Power
- Problems with Steady Power Current
- Power Interference And Preventative Measures
- Environmental Considerations
- Fire Prevention
- Fire Detection
- Fire Types
- Supression Methods
- Fire Extinguishers
- Summary