Certified Information Systems Security Professional, Part 7 of 9: Malware and Business Continuity

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 7 of a 9 part series.

Runtime: 02:33:28

Course description: Malicious software exists in many forms. This course will cover many types of malware including worms, Trojans, viruses along with rootkits and back-doors. It then will cover business continuity, hot and cold sites, redundancy, and backups. Finally it will look at specifics of how to recover from disasters and and how it ties into risk management. This course is part of a series covering the ISC(2) Certified Information Systems Security Professional (CISSP).

Course outline:

Database Models
- Introduction
- Database Models
- Database Models: Hierarchical and Distributed
- Database Models: Relational
- Database Systems
- Database Models: Relational Components
- Foreign Key
- Database Component
- Database Security Mechanisms
- Database Data Integrity Controls
- Add-On Security
- Database Security Issues
- Controlling Access
- Database Integrity
- Data Warehousing
- Data Mining
- Summary

Software Development
- Introduction
- Artificial Intelligence
- Expert System Components
- Artificial Neural Networks
- Software Development Models
- Project Development: Phases III, IV, and V
- Project Development: Phases VI and VII
- Verification vs. Validation
- Evaluating the Resulting Product
- Controlling How Changes Take Place
- Change Control Process
- Administrative Controls
- Summary

Malware Attacks
- Introduction
- Malware Attacks
- Virus
- More Malware
- Rootkits and Backdoors
- DDoS Attack Types
- Escalation of Privilege
- DDoS Issues
- Buffer Overflow
- Mail Bombing and Email Links
- Phishing
- Replay Attack
- Cross-Site Scripting Attack
- Timing Attacks
- More Advanced Attacks
- Summary
- Summary

Project Initiation
- Introduction
- Phases of Plan
- Pieces of the BCP
- BCP Development
- Where Do We Start
- Why Is BCP a Hard Sell to Management
- Understanding the Organization
- BCP Committee
- Summary

Business Impact Analysis
- Introduction
- BCP Risk Analysis
- Identifying Threats and Vulnerabilties
- Categories
- How to Identify the Critical Company Functions
- Loss Criteria
- Interdependencies
- Choosing Offsite Services
- Functions' Resources
- Calculating MTD
- Recovery Point Objective
- Recovery Strategies
- What Items Need to Be Considered in a Recovery
- Facility Backups
- Compatibility Issues with Offsite Facility
- Which Do We Use?
- Choosing Site Location
- Other Offsite Approaches
- BCP Plans Become out of Date
- Summary
- Summary

Disaster Preparation
- Introduction
- Proper Planning
- Executive Succession Planning
- Preventing a Disaster
- Preventative Measures
- Backup/Redundancy Options

(Continued on page 2)

Certified Information Systems Security Professional, Part 7 of 9: Malware and Business Continuity

- Disk Shadowing
- Hierarchical Storage Management
- SAN
- Co-Location
- Other Options
- Summary

Development Plan
- Introduction
- Review: Results from the BIA
- Now What
- Priorities
- Plan Objectives
- Defining Roles
- The Plan
- Types of BC Plans
- Recovery
- Damage Assessment
- Coordination Procedures
- Sequence of Recovery Options
- Relocate to the Alternate Facility
- Restoration of Primary Site
- Return to Normal Operations
- Summary

Emergency Response
- Introduction
- Environment
- Operational Planning
- Emergency Response
- Revieing Insurance
- When Is the Danger Over
- Testing and Drills
- Types of Tests
- What Is Success
- Summary
- Summary