Course ID
SECURITY-EXEC

Course Duration
2-3 days

Course Title
Security, Privacy, and Information Integrity for Managers, Executives, and Policy Makers

Related Courses

- Unified Communications in Public Safety, Law enforcement, and Homeland Security (UNIFIED, 2-3 days)
- State-of-the-art of Wireless Communications for Non-engineering Professionals, Managers, and Executives (WIRELESS-EXEC, 4 days)
- VoIP for 911 Administrators, Managers, Directors and Regulators (VOIP-911, 2-3 days)
- Communications Assistance to Law Enforcement Act (CALEA): Technologies and Compliance for TDM and Packet Voice Services (CALEA, 2-3 days)

Aimed At

Managers, executives, and policy makers at all levels who are concerned with the issues addressed in this course. CEOs often attend the course with the Chief Technology Officers and/or Chief Information Security Officers and members of their security team.

Group Size

5-25

Prerequisites

There are no prerequisites.

Course in a Nutshell

Security, Privacy and Information Integrity are all overlapping areas with different approaches, processes, and outcomes but all can contribute positively or negatively, sometimes in substantial ways, to the organization's value and bottom line financials. This course, based on several years of executive level briefings on the importance and process of organizational "security", is designed to prepare top level executives to make informed decisions about how the handling of information can impact their organization.

The last step of the class will be to review a customizable Organizational Security Report card that will allow the executive to know what to look for and to ask the right questions in assessing the security, privacy, and information integrity of their own organizations. The "Report Card" has been identified as one of the most valuable "take aways" for executives because it allows them to translate thought into action and quickly assess their own vulnerabilities and risks.

Customize It!

We can adapt this course to your group's job functions and concerns at little to no added expense. Let us know how we can tailor this course to your needs.

Course Outline

- Introduction: Network Security Philosophy
  - The Ideal Security System
  - Planning for Internet Security
  - Organizational Security Policy
  - Hacker Profiles and Motives
  - Social Engineering and Reverse Social Engineering
  - The Financial Impact of Network Security
  - The Carrier and Service Provider Security Report Card
- System Security Concepts
  - Encryption/Cryptography
  - Key Management Systems
  - Authentication and Authorization
  - Digital Certificates and Digital Signatures
  - Policy-Based Security Enforcement
  - Malicious Software
- Physical and Infrastructure Security
  - Pass Cards and ID
  - Surveillance Systems
  - Locks and Physical Security Systems
- Network Security
  - Point-to-Point Protocol (PPP)
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)
  - Remote Authentication Dial-In User Security (RADIUS)
  - Tunneling
    - Layer 2 Forwarding (L2F)
    - Point-to-Point Tunneling Protocol (PPTP)
    - Layer 2 Tunneling Protocol (L2TP)
    - Other
  - Internet Protocol Security (IPsec)
  - IP Proxy Agents/Proxy Servers
  - Secure Sockets Layer (SSL)
  - Kerberos

- Anatomy of a Firewall
  - A Sample Firewall: Checkpoint Systems
  - Three Main Operational Areas
    - Security
    - Performance/Availability
    - Policy Enforcement
  - Demilitarized Zone (DMZ) Architecture
- Hacker Tools and Techniques
  - The Insider Threat
  - Exploiting Backdoors, Bugs, and Loopholes
  - Packet Sniffers
  - Social Engineering
  - Reverse Social Engineering
  - Trespassing, Dumpster Diving, and Shoulder Surfing
  - Denial of Service (DoS), Smurfing, and Spam
  - Covert Channels and Steganography
  - Counter-cyberterrorism
- Content Filtering and Monitoring
  - CALEA
  - Content Filtering and Stateful Inspection
  - Filtering and Content Security Overview
  - Privacy and Legal Issues in Domestic and Global Networks
  - Children's Internet Protection Act (CIPA) and Related Topics
  - Types of Filtering: url, content, heuristic, photo, 'sounds like', etc
  - Intrusion Detection System
  - Intrusion Signatures
  - Stateful Inspection
  - Contextual analysis and heuristics
- Disaster Recovery and Contingency Planning
  - Risks to Carrier and Service Provider Infrastructure
  - Disaster Recovery Services
  - Disaster Recovery and Contingency Planning and Drills
  - Disaster Recovery and Business Continuity
- Legal and Regulatory Issues
  - Sarbanes-Oxley (SOX)
  - HIPAA
  - Digital Millennium Copyright Act (DMCA)

- Software Piracy
- Protecting Intellectual Property
- Global Encryption/Cryptography Issues
- Personally Identifiable Information
- Privacy in the Workplace
- Obligations and Liabilities
- Case Law/Case Studies

- The Organizational Security Report Card
  - Report Card Overview
  - Security Self-Assessment
  - Security Report Card Exercise
  - Applying Report Card Results in Your Company
- Conclusion

How You Will Learn

- This course will be taught as a tutorial, consisting of lecture and discussion.
- Your instructor is a highly qualified communications and technologies specialist who's also an expert on security, privacy, and information integrity.
- If you already know something the subject, we will build on that knowledge. If your background is less technical, we will use examples and analogies to make the technical content easier to understand.
- We will provide you with a Participant Handbook that will help you recall and reference what you learned in class.

Revised *May 8, 2008f*