

Who should attend?

The ideal conference for professionals including Data Security Specialists; Information Security Managers and Directors; Information Technology Auditors; Information Technology Managers; Information Technology Planners and Strategists; Security Administrators and Analysts; System Administrators and others with an interest in Network Security & Auditing and Information Risk Management matters.

Program Outline

This conference will deliver the interactive and practical training IT professionals need to expand their knowledge while maintaining their competitive edge. The seminars will feature topics on state-of-the-art practices and management strategies presented by leading information security and network security experts. The format consists of two consecutive in-depth seminars.

Seminar	Topic	CPEs	Member	Non-Member	Dates
1	Information Risk Management	16	\$650	\$800	March 31 & April 1, 2008
2	Network Security Essentials	16	\$650	\$800	April 2-3, 2008
1&2	One person attend both seminars	32	\$1000	\$1300	March 31 - April 3, 2008

Location: OSU - Oklahoma City
900 North Portland Avenue
Oklahoma City, OK 73107
405-947-4421

Amenities: Cost includes seminar, continental breakfast and afternoon snack. Continental breakfast and sign in begin at 7:30 AM; sessions begin at 8:00 AM and end at 5:00 PM.

Agenda:
7:30 - 8:00 Breakfast
8:00 - 12:15 Training Session
10:15 - 10:30 Break
12:15 - 1:15 Lunch
1:15 - 5:00 Training Session
2:30 - 2:45 Afternoon Snack Break

Registration: All registrations and payments must be received by March 3, 2008.

Due to the high demand for the seminar and limited space, participants are encouraged to register as early as possible to reserve a seat. Registration and complete seminar payment must be received by Monday, March 3, 2008. Click the following link or copy and paste the link into your browser.

<http://www.isacacentralok.org>

Please Note:

- Registration is contingent upon full payment of the registration fee. To guarantee your registration, course fees must be received no later than the Monday, March 3, 2008.
- Refunds due to cancellations prior to deadline are paid net of all processing fees. No cancellations can be accepted after Monday, March 3, 2008.
- Substitutions are accepted and encouraged. Substitution of a non-member for a member will result in additional non-member fees being charged.
- The CPEs provided by MIS Training Institute are recognized by the ISACA International organization to meet continuing education requirements for the CISA and CISM certifications.

For questions, please contact Evon Sallee at 405-553-2469 or salleen@oge.com

Seminar 1

March 31 - April 1, 2008

Information Risk Management

Highlights

A Business Perspective on Identifying and Managing Information Security Risks

In today's business climate, information risk management has become a number one priority in most organizations. In addition, new legislation and the best security practices set forth in BS7799 and ISO-17799 point to information risk analysis as the cornerstone of any program designed to safeguard information assets.

In this two-day seminar you will focus on risk analysis and business impact analysis (BIA) as tested methodologies for measuring the level of security risk and prioritizing information risk reduction in your organization. You will explore the fundamentals of each process, build models to fit your individual business needs, and discover how risk management can help you determine if you are meeting the security criteria set forth in HIPAA, GLBA, and Sarbanes Oxley. You will discover how to determine if you need a qualitative method, a quantitative method or a hybrid of the two. You will learn how to create an atmosphere where the information risk analysis process promotes a spirit of cooperation among management, IT, business units and audit. You will master BIA techniques you can use to facilitate managerial risk evaluations that identify the critical business processes and time frames necessary to mitigate disruption and/or loss of data and bring services back to a competitive level. At the end of this intensive seminar you will have built information risk analysis and BIA action plans and put them into practice in real-world scenarios. You are invited to bring actual information risk analysis targets and organizational structures to use in your action plans.

Seminar Outline

1. Information Risk Management

- four phases of information risk management
- how the information risk management process fits into the information protection program
- integrating risk management into an enterprise-wide process
- partners in the information risk management process and the roles of each one
- moving from centralized to decentralized information processing

2. Information Risk Analysis

- the risk analysis cycle and its components

Outline

- management's concerns and perception of the information risk analysis process
- types of information risk analysis: quantitative vs. qualitative approach
- software tools for performing the information risk analysis process
- identifying asset categories: IT, business processes, or business functions
- defining information risk analysis targets and scope
- statements that create boundaries for the information risk analysis process
- the information owner's role in the information risk analysis process

3. Developing an Action Plan You Can Implement

- administrative information required in the action plan
- logging risk and control information
- creating action items in response to identified controls
- using the action plan for an approval process
- how the information risk analysis action plan is distributed and protected

4. Assets, Risks, Threats, and Vulnerabilities

- identifying assets in an information risk analysis
- determining asset values
- prioritizing, categorizing, and documenting information risks
- uncovering information vulnerabilities

5. Management Decisions

- arriving at an "acceptable level of risk"
- identifying controls in an information risk analysis
- determining the cost of control
- categorizing and documenting information controls for a total program

6. Control Implementation

- using the action plan to create assignments, schedules, and approvals
- involving auditing in the process

7. Follow Up

- tracking the information risk analysis process: start to finish
- enforcing the use of the information risk analysis process

8. Business Impact Analysis

- business impact analysis process: components and definitions
- BIA as the key to a successful data security program
- partners in the business impact process and the role each one plays

Speaker Profile

9. Developing a BIA Action Plan

- administrative information required in the action plan
- identifying "impact criteria" and their importance to the organization
- pinpointing key business processes and peak activity periods
- developing algorithms to calculate business losses
- distributing and protecting the business impact analysis action plan

10. Using the Business Impact Analysis

- creating the prioritized applications list
- building organizational disaster recovery and business continuity plans using the business impact analysis results.

Speaker: Ken Jaworski, CISSP

Ken Jaworski is a Project Manager for Compuware Corporation, where he is responsible for a variety of assignments in both the public and private sectors. His areas of expertise encompass information security policy development, business resumption and disaster recovery planning (including business impact analysis), risk management, using the ISO-17799:2005 framework as in infosecurity management structure, and data classification and security. In addition, he is well versed in legal and industry security mandates as set forth in such legislation as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley, and SB1386.

Prior to joining Compuware, Mr. Jaworski had a 31-year career with Detroit Edison. While at Detroit Edison, he worked in the information protection organization and helped build the 1996 Information Protection Program of the Year. Mr. Jaworski was a contributor to the application development and controls organization for more than 18 years.

With MIS Training Institute since 1996, Mr. Jaworski is the primary instructor for MIS' Information Risk Management, Data Privacy, and Business Continuity Planning seminars. He also provides instructor support for other MIS management-level information security courses, and serves as a sector chairperson for MIS'IT Security World conference.

CPEs: 16

Seminar 2
 April 2 - 3, 2008

Network Security Essentials

Highlights

Outline

Speaker Profile

A Comprehensive Introduction to Network Control Points and Associated Safeguards.

In this two-day seminar you will review the basics of LANs, WANs, client/server and other forms of distributed computing architectures. You will survey the security and audit features of network operating systems, interconnection devices, remote access methods, and add-on security products. You will also map the use of security features to security policy requirements to determine the topics that must be addressed in developing security administration standards and procedures, and designing self-assessment plans. (Note: This seminar covers the topics found in Chapters 3 and 4 of the CISA Review Manual.)

Seminar Outline

1. Defining the Distributed Information Technology Environment

- defining a network
- network terminology
- computing models: centralized and distributed
- shared data networks
- client/server computing
- peer-to-peer applications
- defining the scope of network security and audit programs

2. Network Standards and Protocols

- protocol defined
- network communications standards
- rules for communications
- Open Systems Interconnection (OSI) Model
- common network protocols
- Transmission Control Protocol/Internet Protocol (TCP/IP)
- analyzing the OSI layers
- geographical network delineation: PAN, LAN, WAN
- untangling the 'Nets: Internet, intranets, and extranets

3. Local Area Network Connections

- common network transmission media: twisted pair copper wire, fiber optics
- physical network topologies: bus, ring, star, tree
- logical topologies: Ethernet, Token Ring, FDDI, ARCNet, LocalTalk
- backbone networks
- wireless local area and personal area networks

4. Wide Area Network Connections

- WAN and Internet connections
- dial-up Internet connections
- switching techniques

- leased digital line services
- packet routing services
- residential broadband

5. Network Devices: Functionality, Management and Security

- positioning network devices in the OSI Reference Model
- network interconnection devices: Layers 1 and 2
- network domains and segmentation
- network interconnection devices: Layers 2-7
- network device maintenance port access
- Simple Network Management Protocol (SNMP)

6. Performing a Network Security Risk Analysis

- determining the security of your network
- identifying assets
- categorizing threats
- analyzing current threats to network security
- tracking network security vulnerabilities
- network vulnerability testing
- defining a network security strategy

7. File Server Security and Audit

- LAN security control points
- server vulnerabilities
- security mechanisms
- server security baseline checklist
- server operating system security features and deficiencies: Microsoft Windows NT/2000, Unix variants, Novell NetWare
- add-on security features
- server auditing tools and techniques

8. Workstation/Client Security

- workstation security challenges
- workstation access control
- Windows file shares
- viruses and other malicious software
- auditing workstation security

9. Network Perimeter Security

- hacker intrusion objectives
- network security strategies
- warning banners
- network firewalls
- intrusion detection systems
- remote access/dial-up access security
- VPNs

10. Directory Services Security and Audit

- overview of Directory Services
- Lightweight Directory Access Protocol (LDAP) directories
- Domain Name System (DNS)

11. Wrap-Up: Network Security Strategies

- defining "perfect" network security
- a practical strategy for information security
- 12-point plan for success

Speaker: Martin Green

Martin Green is a senior instructor for MIS Training Institute. A member of the MIS faculty for more than 20 years, his areas of expertise include computer technology, networking, and security. Mr. Green also maintains an active consulting practice to lawyers and other professional service businesses regarding office automation and related auditing and security issues.

Mr. Green leads several technology courses for MIS, including Auditing Networked Computers and Network Security Essentials. In addition, he is a frequent speaker at the MIS Annual Conference and Expo on Control and Audit of Information Technology.

CPEs: 16