

The Cyber Threat: A Seminar/Workshop for Audit Professionals

This is a one-day seminar that gives financial and IT auditors a sound introduction to the realities of the threats of cyberattacks. It provides them with an understanding of what such attacks mean to business and what they can do to support prevention, detection and, most important, business recovery should such an attack occur. The class combines lecture with hands-on exercises. It focuses on the role auditors can play in assuring that their organizations are taking appropriate measures to protect themselves from cyberattacks.

Intended audience: Internal and External Financial Auditors, Internal and External IT Auditors, Risk Managers, Business Managers, Financial Executives

Learning objectives: Participants in this seminar will learn:

- How the reality of cyberattacks fits into their business models
- How cyberattacks occur and what can be done to stop them
- Audit objectives and techniques regarding cyberattacks
- The pros and cons of cybersecurity products in the marketplace
- Audit's role in the organization and governance of cybersecurity
- Building a culture of cybersecurity
- How to detect and recover from a cyberattack

Seminar outline:

- A. Cyberattacks – Myth and Reality
 - a. Different types of attack and response
 - b. The scope of the problem
 - c. Effects on business
 - d. Shortfalls of existing organizational preparations

- B. How the Threat of Cyberattacks Can Be Mitigated
 - a. Basic Do's and Don'ts
 - b. Safeguards in place
 - c. Potential weaknesses
 - d. Secure architecture
 - e. Attack vectors

- C. Audit's Role in Cyber Security
 - a. Audit's role
 - i. Oversight and information
 - ii. Adhering to best practices
 - iii. Supporting appropriate investment
 - iv. Assuring that others are fulfilling their roles
 - b. Audit approaches
 - i. Standards-based
 - ii. Experience based
 - iii. Testing-based

- D. Organization and Governance
 - a. Board of Directors
 - b. Computer Emergency Response Team (CERT)
 - c. Crisis Management Team (CMT)
 - d. Information Security
 - e. Business Continuity Management
 - f. IT functions
 - g. Business functions
 - h. *Workshop exercise*

- E. Solutions in the Marketplace
 - a. Cybersecurity products
 - b. Insurance
 - c. *Workshop exercise*

- F. Cyberattack Detection
 - a. Human factors
 - i. Training and attentiveness
 - ii. Presumption of a hostile environment
 - iii. Dealing with false alarms
 - b. Recognizing an attack is under way
 - i. Signature recognition
 - ii. Anomaly detection
 - c. Heuristics
 - d. Alerts, alarms and triggers
 - i. Unusual volume
 - ii. Slow response times
 - iii. Unanticipated changes to software
 - e. Statistical models

- G. Cyberattack recovery
 - a. Resources
 - i. Trusted images
 - ii. Clean storage environment
 - iii. Recovery environment
 - 1. Recovery in place
 - 2. Standalone environment
 - b. Planning
 - i. Planning variables
 - ii. Recovery timing
 - c. Recovery steps
 - d. *Workshop exercise*

H. Conclusion

Seminar logistics: This is a one-day seminar/workshop (8 CPE hours). Because of the intensive case study workshop, the seminar attendance should be limited to approximately 40 people.

Contact:

- Steven Ross, Executive Principal, stross@riskmastersintl.com, (917) 837-2484
- Stacy Olewiler, Associate Principal, solewiler@riskmastersintl.com (717) 368-6256