RMI Risk Masters International LLC

Prevention, Detection and Recovery from Cyberattacks
A Seminar/Workshop

This is a two-day seminar, combining lecture with a hands-on, case-study based workshop that introduces individuals responsible for dealing with cyberattacks to the principles and practice of prevention, detection and recovery from hostile actions against computer systems. It includes both the technical and organizational measures that are required and focuses on the steps that must be taken and the skills that must be obtained in advance of an attack to be prepared should one occur.

Intended audience: Information Security managers and staff, I.T. management, technical support and operations personnel, Disaster Recovery Planners, Business Continuity Managers, I.S. Auditing managers and staff, Corporate Management, Risk Managers and staff

Learning objectives: Participants in this seminar will learn:

- How the reality of cyberattacks fits into their business models
- How to organize, build and maintain an effective capability to prevent, detect and recover from cyberattacks
- What tools, skills and techniques are needed to support cyberattack response
- How to test and validate recovery capabilities
- What architectural and design alternatives can be applied for cyberattack prevention, detection and recovery
- How cybersecurity can be governed and managed

Seminar outline:

A. Cyberattacks – Myth and Reality
    a. From hacking to attacking
    b. State-sponsored attacks
    c. Criminal attacks
    d. The threat, current and potential
    e. Why existing Disaster Recovery Plans are insufficient

B. Organization and Governance
    a. Computer Emergency Response Team (CERT)
    b. Crisis Management Team (CMT)
    c. Information Security
    d. Business Continuity Management
    e. IT functions
    f. Business functions
    g. Case study

C. Building a CERT

a. Management support and funding
b. Key stakeholders and participants
c. Mission, roles and responsibilities
d. Resource requirements
    i. Personnel
    ii. Software tools
    iii. Hardware
    iv. Emergency communications
e. Procedures
f. Training
g. Testing and validation
h. Case study

D. Cyberattack Prevention
    a. Architecture and design
        i. Networks
        ii. Servers
        iii. Data storage
    b. Safeguards
        i. Firewalls
        ii. Antivirus filters
        iii. Intrusion detection and prevention systems
        iv. Software to enforce proper behavior
    c. Training
        i. CERT
        ii. Help Desk
        iii. End users
    d. Maintenance
        i. Change Control
        ii. Upgrades
    e. Case study

E. 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
    f. Case study

F. 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. Case study

G. Assessing and auditing cyber-response capabilities
a. Standards-based
b. Experience based
c. Testing-based
d. Involvement across an enterprise
e. Case study

H. Conclusion

Seminar logistics: This is a two-day seminar/workshop (16 hours). Because of the intensive case study workshop, the seminar attendance should be limited to approximately 35 people.
Contact:

Steven Ross, Executive Principal, stross@riskmastersintl.com, (917) 837-2484

Stacy Olewiler, Associate Principal, solewiler@riskmastersintl.com (717) 368-6256