

Cyber Terrorism & Electronic Espionage

COURSE DURATION: 2-days

CPE HOURS: 16

LEVEL: Intermediate / Group-Live

PREREQUISITES: None

ADVANCE PREPARATION: None

The 21st century has arrived and with it a new electronic world that poses significant business risks. Global terrorists know that winning a physical conflict with the major world powers is virtually impossible. They have now discovered that critical commercial infrastructure is highly exposed to a logical attack, therein jeopardizing our society and way of life. The list of potential targets includes power grids, banks, airlines, air traffic controls systems, trucking and transportation companies, chemical and petrochemical facilities, food manufacturers, retailers, hospitals, and local governments. Many of these organizations do not have the necessary controls to detect and repel a serious penetration attempt as the Canaudit Penetration Team has repeatedly proven in client after client. The controls are just not in place to protect most organizations from electronic warfare or terrorism. Electronic espionage also poses a significant threat as cyber criminals are creating new ways to earn a living. Penetrating networks, harvesting files, deleting or altering critical databases, and taking control of critical network components are just a few of the risks.

This highly intensive seminar will provide you with an understanding of the specific risks related to Cyber Terrorism and Electronic Espionage. You will also receive an audit guide containing a series of checklists and risk control tables to help you perform a threat assessment of your own organization.

WHO SHOULD ATTEND

This session is intended for auditors, security, and law enforcement professionals interested in identifying the specific electronic threats to their organization's information technology.

SEMINAR OUTLINE

I What is Cyber Terrorism?

- Objective of Cyber terrorism
- Who are likely perpetrators?
- Is it as easy as they say?
- How would they do it?
- Live demonstration
- Preliminary targeting
- Planning the attack
- Could it really succeed?

II What is Electronic Espionage?

- Definition & explanation
- The impact of open systems
- Understanding the risk
- Types of Electronic Espionage
- Electronic storage facilitates theft
- Internal penetration by trusted employees
- External penetration
- Examples of poorly secured machines
- Live demo of hacker tools
- Identification of valuable data by application

III What Can We Do?

- Basic housekeeping
- Hardening the network
- Preemptive security
- Penetration audits
- Protecting data
- Gathering knowledge

IV Is Your Company Truly at Risk?

- Common misconceptions
- The obvious, secondary and forgotten targets
- The forgotten targets
- Getting management's attention and funding
- Risk Control Tables
- Control checklists

V Points of Penetration

- Identifying Points of Penetration
- Identifying connectivity
- Scanning the network
- Identifying unauthorized connections to other networks
- Using exploits to prove risk

- Performing a modem hunt or demon dial
- Exploiting the Internet connection
- Beating the firewall
- Trading partner issues
- Third party & general attacks
- Remote control programs: the terrorist's friend
- The internal attack
- Employees & contractors
- Temporary staff can be plants

VI Preventive and Preemptive Controls

- Prevention & readiness
- Installing preventive controls
- The network: first line of defense
- Securing NT and UNIX
- Watch out for sniffers
- Protect your email

VII Conclusion