

Educational Opportunities

Emerging Cyberthreats and Countermeasures **Internet Security Presentation and Intrusion Prevention Workshop**

“Emerging Cyber Threats and Countermeasures” is a timely review of the current threat environment. It includes the most important information from many of our network security workshops, including “Hacking Through a Firewall”, “Anatomy of a Browser Attack”, and “The Top 10: A Review of the Latest Exploits”. Learn about the current top attacks and how they function: cross site scripting, injection flaws, malicious file execution, brute force logon attempts, and buffer overflows are just a few of the current attacks covered in this informative and up-to-date report on the latest tactics the “bad guys” are using with unprecedented frequency.

The Presenter



David A. Lissberger is founder of EcoNet.com, Inc. and serves as the president and CEO of the firm. EcoNet.com is one of Dallas’s oldest Internet application development firms and the inventors of Network Cloaking™ technology. EcoNet.com manufactures the Sentinel IPS, a network Intrusion Prevention System (IPS), which protects private networks from hackers and malicious activity through their Internet gateway.

In 2004, EcoNet started selling the first commercial versions of this technology under the name of Sentinel IPS. Since that time, Sentinels have been installed across the US, Canada and Europe. Clients include Fortune 100 firms, industry, government, and small business. Sentinel IPS devices currently defeat approximately 100 million intrusion attempts per month.

David holds an M.B.A. in International Marketing and Finance from Southern Methodist University Cox School of Business and a B.A. from Texas A&M University. He is an avid private pilot and a Texas real estate broker.

Target Audience

Professional organizations, CEOs, CIOs, CFOs, COOs, CSOs, IT Directors, Network Engineers, Security Compliance Officers for HIPAA, SarBox, GLB, & ISO 17799.

Continuing Education for lawyers, accountants, real estate and other professionals.

Law enforcement organizations, federal, state, and local governments, military, Homeland Security, and universities.

Time Requirements

30 to 60 minutes, Q&A optional.

Equipment Requirements*

Projector and laser pointer, sound system with 1/8” input, sound system with microphone for audiences of 25 or more, white board and dry erase markers for more technical audiences. Multiple monitors may be required for audiences over 100.

Reimbursement Requirements

Generally, only reimbursement for travel is requested, however travel outside the United States may require an honorary.

** Please make prior arrangements if equipment is not available*

Most organizations are vulnerable to being hacked because they simply do not understand how vulnerable they may be, or they believe protection is too expensive.

This presentation shows how vulnerable networks may be compromised and offers new ideas, such as Network Cloaking, Pre-Emptive Attack Mitigation, remediation techniques, tips, and helpful suggestions that network administrators and corporate officers should consider to make their network environments more secure.

Previous Audiences

AFCOM
US Secret Service
North Texas Global Telecom Society
Texas Society of CPAs
Greater Dallas Board of Realtors
Texas Association of IT Managers
Vanguard Security Conference
Texas Bankers Association
Association of IT Professionals
Hi-Tech Electronic Crimes Task Force
Department of Homeland Security