Moderator: Kristen Zarcadoolas, Director

Panelists: 
- Judi Flournoy, CIO
- Don Jaycox, US CIO
- Kenneth G. McGuire, Supervisory Special Agent
- Jim Soenksen, CEO
Discussion Objectives

- Firm Dynamics, IT Environment, and Major IT Initiatives
- 2005 Information Security Initiatives, Solutions, and Recommendations
- Cyber Crime Incident Handling and How to Work with Law Enforcement
- Top Ten Law Firm Security Issues
- How to Make Information Security a Business Enabler for Your Firm through Best Practices
Loeb & Loeb LLP

Judi Flournoy
CIO
Firm Demographics

• 200 Attorneys, 500+ Users
• Four locations
  • Los Angeles – main office
  • New York – second largest office
  • Chicago
  • Nashville
IT Environment

- Windows 2000/2003 Server
- Windows 2000 Professional
- Office XP
- Postini – Spam & Anti-Virus
- Trend – Anti-Virus and Personal Firewall
- AdAware/AdWatch
- RSA Server 6.0
Major IT Initiatives

- EMC Storage Area Network
- FalconStor
- Electronic Records Management
- Disaster Recovery
- Wireless LAN
2005 Security Initiatives

- Citrix MetaFrameXP
- Juniper NetScreen 1010
- Firewall Upgrades
  - Cisco PIX or Juniper
“Security” @ Loeb

- Security is something we take seriously
- Users are expected to partner with us in assuring our resources are secure
- Firm policies support the concept of network security
- We are conscious of the profile of some of our clients and are particularly sensitive to the need to protect them
Additional Tools We Use

• Snort
  • http://www.snort.org
• QualysGuard Enterprise
  • http://www.qualys.com
• Nessus
  • http://www.nessus.org
Wireless @ Loeb

- Treo 600 & Treo 650
- GoodLink 100
- Blackberry
Connecting Remotely

- Via Internet
- Via Dial-up using iPass or 802.11x via iPass Hot Spots
- Two factor authentication
- SSL Encryption
Remote Access @ Loeb

User accesses Loeb remote

http://

User is prompted for credentials

User obtains token

User is authenticated

User accesses resources
Future Wireless LAN

- WiFi access points on all floors
- Authentication via Certificate Based
- Use of VLAN’s to segregate visitor traffic
Security & Recommendations

- Have someone on staff responsible for security or hire a third party
- Force password changes
- Force strong passwords
- Use 2 Factor Authentication
- Periodically test vulnerability
- Do not permit outsiders on your network
  - Secure your wireless
What Questions Do You Have?
DLA Piper Rudnick Gray Cary
Firm Demographics

- Result of 3-way merger on Jan 1, 2005
- 1400 attys, 3100 people in the US
- 2800 attys, 6000 people worldwide
- 26 US offices, 50 Worldwide offices
IT Environment

- Win 2K / Win2K3 Server, AIX (Unix)
  - 1000’s of servers worldwide
- Win XP (SP1/SP2) desktop / laptop
  - Most attorneys carry laptops
- Office 2003 w/ mixed Worksite / PC Docs
- Support 600+ home offices in US
- Support 1000+ roaming users
- Heavy use of Collaboration systems
DLAPRGC Security Environment

- Postini / FrontBridge anti Spam
- Trend eWall (SMTP GW policy server)
- Checkpoint & Cisco firewalls, VPN/PFW
- McAfee w/ EPO virus protection
- PestPatrol - Spyware
- Rolling out Cisco Security Agent (CSA)
- Managed Security Services thru LURHQ
  - FW, IDS, IPS, advisories, threat assessment
Wireless

• Most attorneys (90%) carry BB 7230 o.e.
  • 4 BES servers, email, web / intranet access
• 35%+ home offices have wireless
• 500+ attorneys use roaming WiFi Hspots
  • TMobile, Boingo, Wayport mostly
• All large offices wired for guest WiFi
  • Most other offices in lobby & conf rooms
• Must be running Checkpoint or Cisco VPN/PFW to get WiFi access
Remote Access

- Broadband - Home, hotel, client sites
- Wireless - Home, wifi hotspot, client wifi
- Dialup - Cisco modem server w/ RSA
- Checkpoint & Cisco SW VPN
- Some NS5XP appliances (phasing out)
- Citrix
- OWA (mixed -- may phase out)
IT Priorities - 2005+

- Merger, Merger, Merger...
  - Many differences in policy & practice
  - New offices, New laterals
- Consolidate systems ...
  - Elite, HR, email, AD, DMS, RMS, docket, etc.
- Data center consolidation
  - From 25 US locations down to 3
  - SAN & over-the-wire backups
- Major Expansion of ...
  - Collaboration systems, remote access
Security Posture

- Educated user community: best weapon
  - Skepticism: most important tool
- Security is everyone’s responsibility
- Mobile work force invalidates “citadel” model - Alternative: “cargo net” model
- User communication / Policies -
  - Passwords, Phishing, email scams, encryption, confidentiality
What Questions Do You Have?
Federal Bureau of Investigation

Kenneth G. McGuire
Supervisory Special Agent
Topic Overview

1. Current Security Threats & Cases
2. Cyber Crime Incident Handling
3. Working With Law Enforcement
Security Threats & Cases

1. TYPES OF PERPETRATORS
2. INTERNET FRAUD - Identity Theft, Phishing Schemes, Remailer Schemes
3. COMPUTER INTRUSIONS & DISRUPTIONS –
   1. RATs (Remote Access Trojans),
   2. Extortion by DDoS (distributed denial of service),
   3. “Hacker for Hire” Investigation,
   4. Wireless Networks Concerns
4. INTELLECTUAL PROPERTY RIGHTS CRIMES –
   Warez/Movie Servers
How Severe is the Threat?

- Professional Cyber Criminals & Terrorists (hard to detect)
- Disgruntled Employees
- Competitors
- Hacktivists
- Script Kiddies (Advertises Actions)
Identity Theft

• Growing sophistication of phishing emails
• Exploitation of Banking System
• Keystroke Loggers deployed by worms
• Exploding International Market for Stolen Credit Card Databases and Identity Data
• FTC - $50B lost in Identity Theft in 2003
• 300M man-hours devoted to repairing damage caused by this theft
Growing Trends

- Virus/Worm Payloads Used to Facilitate Intrusion/Fraud Schemes
- Mercenary Distributed Denial Of Service Attacks
- Extortion Schemes Fueled by DDOS and Intrusion
- Identity Theft Underpins Most Computer Crime
- Overall increase in sophistication by a geographically diverse criminal element
Banking and Brokerage Account Compromise

• Driven by worm propagation with keystroke logger in payload

• U.S. citizens recruited to open bank accounts for 30% fee

• Funds first transmitted to other U.S. accounts, then to the Eastern bloc.
REMOTE ACCESS TROJANS (RATs)

• HACKER versions –
  Subseven, Backorifice, Netbus
  • Sometimes contained in email or programs downloads, i.e. P2P programs like Kazaa

• COMMERCIAL PROGRAMS –
  GotomyPC, PC Anywhere, Laplink

• OPERATING SYSTEMS PROGRAMS –
  Telnet, ftp, Secure Shell (SSH), rlogin
World’s Largest Computer Equipment Supplier

• A union of computer intrusion and wire fraud
• Subjects have placed at least $10M in fraudulent orders
• Subjects use work-from-home web sites to recruit unwitting U.S. participants
• 11 convictions to date in the U.S., at least a dozen to follow
Extortion By DDOS

- Hiring hackers to create distributed denial of service (DDOS) attacks
Countermeasures

- Practice good computer security
- Invest in a personal shredder
- Examine your credit report annually
- Scrutinize credit card statements
- 1-888-5-OPTOUT (1-888-567-8688)
- Use caution supplying wire transfer info
- Be alert to anomalous personal info requests
- http://www.consumer.gov/idtheft/
Wireless Security Concerns

1) Availability of free WAP detection and logging tools like Netstumbler and Kismet

2) War Driving—where individuals drive (or walk) around to find unprotected and accessible WAPs

3) Consumer and even system administrators fail to configure their systems adequately
Wireless Security Measures

Wireless Encryption Protocol
or
Wireless Equivalency Protection (WEP)

1. Uses 128-bit encryption

2. WEP uses weak algorithm that has been broken and is available to hackers

3. Replacement for WEP called WiFi Protected Access (WPA) not widely implemented

4. WEP is not configured out of the box and therefore, not protecting the system

5. When WEP is configured by owner the default password is used - ADMIN
Preventing Disgruntled Employee Problems

• Terminating System Access BEFORE TERMINATED EMPLOYEES ARE WALKING OUT THE DOOR
• Well Documented and Proliferated Non-Disclosure and Authorized Activity Agreements/Notifications
• Review Adequate Logging/Tracking
• Enforce Your Rules
• PRACTICE EXERCISE – “RED TEAMING”
• BANNER during Log-in of company computers
2. Identify the Incident Manager and Team – usually department heads or officers
3. Assess Systems Impaired and Damages
4. Review Adequate Logging/Tracking
5. Note Unusual Activities By Employees or on Computer Network
WORKING WITH LAW ENFORCEMENT

- Identify your LOSS, HARM, or DAMAGE – lost asset, revenues, expenses, repair cost
- Identify Capture or Quarantine Electronic or Computerized Equipment, Logs and Files
- Maintain a “Chain of Custody” for Evidence
- Begin a written chronology of events
- Who may have to testify
- Identify one or two individuals to be your main point of contact with LEOs
- Alert Your General Counsel or Atty
WORKING WITH LAW ENFORCEMENT

• CRIMINAL LAWS THAT APPLY:
  – ECPA (Electronic Communications and Privacy Act)
  – 4th Amendment – Search & Seizure
  – Interception of Communications (Wiretapping)
  – Court Orders – FGJ Subpoenas, Search Warrants, Pen Registers, Trap & Trace Orders, 2703(d) Orders, Title 3 Orders
Prepare for Incident Response

• Have A Disaster Plan for Human-made and Natural Disasters
  – Need some ideas, try Risk Management Organizations

• Practice The Plan!

• Review The Plan Annually!
  – Include contacts with law enforcement or disaster officials
INFRAGARD PROGRAM

Government Operations
Emergency Services
Telecommunications
Electrical Energy
Transportation
Gas & Oil Storage and Delivery
Water Supply Systems
Banking & Finance
Contact

INFRAGARD COORDINATOR
Regina Miles-Canales
310-477-6565
Contact

Cyber Crime Supervisor
Ken McGuire
310.996.3854
kenneth.mcguire@ic.fbi.gov
What Questions Do You Have?
Pivot Group
Crystal Ball Wrap-Up

Jim Soenksen
CEO
Top Ten Security Concerns

1. Security Updates
2. Spam
3. Spyware
4. Remote Access
5. Wireless
6. Roaming Laptops
7. VOIP
8. Data Privacy and Protection
9. Proactive Security Program
10. Training & Education
Defense In-Depth

- Defensive Wall 1:
  Blocking Network Attacks
- Defensive Wall 2:
  Blocking Host Attacks
- Defensive Wall 3:
  Eliminating Security Vulnerabilities
- Defensive Wall 4:
  Safely Supporting Authorized Users
- Defensive Wall 5:
  Tools to Minimize Business Losses & Maximize Effectiveness
Embrace Best Practices

look, plan, act, repeat

Proactive Security is Less Expensive than Reactive Security!
Emerging Security Technologies

- Biometrics
- Behavioral Based
- VOIP Protection
- Regulatory Compliance
- Business Back Up & Recovery
- Wireless Protection
- Forensics
- e Discovery
- Privacy
Helpful Sites

- [http://www.sans.org/top20/](http://www.sans.org/top20/)
- [http://cert.org/](http://cert.org/)
- [http://www.infragard.net](http://www.infragard.net)
- [http://www.gosci.com](http://www.gosci.com)
- [http://www.pivotgroup.net](http://www.pivotgroup.net)
Final Questions
Thank You
from
Judi Flournoy, Don Jaycox, Ken McGuire, Jim Soenksen, and Kristen Zarcadoolas