Emerging Trends in Information Security

May 18, 2004

Kris VanBeek
Federal Reserve Bank of Boston
Kris.vanbeek@bos.frb.org
Presentation Focus Areas

- Technology Risk
- Technology Risk Assessment
- Emerging Risks
- Example Discussion
Recent Events

- SASSER (A,B,C,D)
- BugbearB (targeted certain small banks)
- Phishing
- Many Local and Regional Bank Events
- Acxiom (impacted banks & California law)
- Many, many, others
Threat Evolution

- Viruses
- Network Intrusions
- Blended Threats (Code Red, Nimda)
- Denial-of-Service (Yahoo!, eBay)
- Mass Mailer Viruses (Love Letter/Melissa)
- Zombies
- Polymorphic Viruses (Tequila)

Number of Known Threats:
- 70,000
- 60,000
- 50,000
- 40,000
- 30,000
- 20,000
- 10,000

Timeline:
- 1987
- 1988
- 1989
- 1990
- 1991
- 1992
- 1993
- 1994
- 1995
- 1996
- 1997
- 1998
- 1999
- 2000
- 2001
FBI Banking Intrusion 2003

2003 - the FBI has a record number of cases involving:
- bank intrusions
- theft of customer account information
- Malicious code

The intrusions used various exploits against known vulnerabilities:
- Unicode Internet Information Service Exploit (IIS)
- Redirecting Customers to Websites
- Blended threat attacks that include Remote Access Trojans
Bugbear A 9/02 and Bugbear B 6/03

- Propagation via email
- Propagation via local area network shares
- Trojan Backdoor- remote command and control of victim system
- Trojan Keylogger - Logs and Exfiltrates personal information (i.e. credit cards, SSNs)
- Email information to multiple dropsites
- Deletes antivirus and security programs
- Targeted the Financial Community
Bugbear B

- 270,000 machines infected with Bugbear.B within the first two hours of proliferation

- First worm that targeted the Financial sector 1,500 banks’ IP hard coded into the code

- Personal Information Stolen
  - Hundreds of thousands of credit card numbers
  - Social Security Numbers
  - Login and passwords (Keystroke logging)
  - Screen captures
Threats

- Threat Sources
  - Insiders (FI & vendor) remain greatest threat
  - Hackers: malicious, casual, or opportunistic

- Targets
  - Confidential Information
  - Banking Assets
  - Reputation
Types of Threats

- Unauthorized access (internal & external - many types social eng.)
- Viruses, Worms, Trojan Horses, etc.
- Web site modifications
- Web site spoofing/phishing
- Denial of Service attacks
- Theft of confidential/proprietary information
- Possible extortion attempts
Why Do You Care?

Safeguarding Customer Information

GLBA
501 b
Primary Categories of Risk

IT & Internet Risks

- Credit
- Liquidity
- Interest Rate
- Price
- Reputation
- Strategic
- Transaction
- Foreign Exchange
- Compliance
Risk Management Process

- Identify
- Measure
- Control
- Monitor

Effective Risk Management
CIA Security Model

A well conceived and implemented security program should confirm

- Confidentiality of Data
- Integrity of Data
- Availability of Data
What’s Happening

● Lack of risk assessment
● Ability to identify an event?
● Process once an event identified?
● Established priorities?
What’s Emerging

- Worm/virus
- Phishing
- Targeted attacks
- Morphing
- Lower level targets
- Technical people & criminal
- Identity theft
What To Do

• Talk before it happens
• Method of identifying an event
• Define priorities
• Have a strategy and written plan
• Awareness/Education
• Patch and vendor management
Update to the handbook is an ongoing process

Many booklets have been issued, but will be regularly updated
Guidance Booklets

Outsourcing
Information Security
Business Continuity
IT Audit
IT Operations
Networks/Connectivity
Payment Systems: Fedline
Payment Systems: retail
Payment Systems: Wholesale
Electronic Banking
Many Others
Contact

Kris VanBeek, Supervisory Examiner
Federal Reserve Bank of Boston
600 Atlantic Avenue - PO Box 2076
Boston, Massachusetts 02106
(617) 973-5976  kris.vanbeek@bos.frb.org