OCC 99-9

Subject: Infrastructure Threats from Cyber-Terrorists
Description: Message to Bankers and Examiners
Date: March 5, 1999

To: Chief Executive Officers and Chief Information Officers of All National Banks, General Managers of Federal Branches and Agencies, All Department and Division Heads, and All Examining Personnel

PURPOSE

The purpose of this bulletin is to identify and raise awareness of the threats and vulnerabilities created by cyber-terrorism to the financial services industry. OCC's concern is with how rapidly the threats from terrorists and criminals are evolving in terms of technology, and our banks' ability to develop and implement adequate preventive controls and countermeasures. This bulletin does not represent a change in OCC policy. It is meant to heighten visibility of this issue, discuss our concerns, and highlight the importance of our financial institutions' ability to protect the integrity, confidentiality, and availability of their information resources.

CONTENTS PAGE

SUMMARY OF KEY POINTS

Cyber-terrorism is the use of computing resources against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. These can be operations to disrupt, deny, corrupt, or destroy information resident in computers or available via computer networks.

Cyber-terrorists can be an individual, a criminal organization, a dissident group or faction, or another country. Attacks can be generated internally or externally, and may be directly against a computer system, or focus on the supporting infrastructure (telecommunications, electricity, etc.).

As used in this document cyber-terrorism includes acts of

commercial espionage and employee sabotage.

Cyber-terrorism can be one catastrophic attack on our infrastructure, or a series of coordinated, seemingly independent attacks. This latter point emphasizes the importance of reporting suspected cyber crimes and computer intrusions on Suspicious Activity Reports (SAR) (see OCC Advisory Letter 97-9), in order for OCC and other agencies to identify patterns that might comprise a coordinated systemic attack. The federal computer crime law is 18 U.S.C. 1030.

Penetration attempts or actual damage caused by seemingly isolated computer security incidents can spread to other systems, causing widespread denial of service and other losses.

Vulnerabilities to cyber-terrorism can be managed using a variety of cost-effective countermeasures readily available.

Information technology is sure to proliferate, and those who would exploit it for nefarious purposes are sure to multiply.

BACKGROUND

Prior to the 1990s, the predominant threats to computer security of financial institutions (besides errors and omissions) were physical and environmental, including insider attacks, fire and water damage, theft, and physical damage. The primary sources of such threats were frequently authorized users or insiders. The bank regulatory agencies and regulated financial institutions focused their efforts on the deployment of sound internal controls to alleviate those threats. Those threats are now largely understood and controllable through the use of traditional controls and contingency planning.

Cyber-terrorists pose related and arguably more significant threats to this nation's financial institutions, as well as other parts of the nation's infrastructure. These threats include the use of computer viruses, network worms [Network worm - a program that scans a system or an entire network for available, unused space in which to run. Worms tend to tie up all computing resources in a system or on a network and effectively shut it down.], and Trojan horses [Trojan horse - a program that appears to perform a useful function and sometimes does so quite well but also includes an unadvertised feature, which is usually malicious in nature.].

As commercial technologies create advantages, their increasingly indispensable nature transforms them into high value targets of cyber-terrorists and cyber-criminals. The Year 2000 problem has served to heighten the awareness of our nation's critical reliance on technology and permeates all industries through the interdependence of our infrastructures. These critical infrastructures include telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both government and private.

Recent advances in computer hardware, software, and communications technologies have made these infrastructures highly automated and capable.

While technological advances have promoted greater efficiency and improved service, they have also made these infrastructures potentially more vulnerable to disruption or incapacitation by a wide range of physical or computer-based (cyber) threats. The infrastructures are much more interdependent than in the past, with the result that the debilitation or destruction of one could have cascading destructive effects on others. Electronic transactions within the financial services infrastructure underpin the entire national economy, as well as the operations of the other infrastructure sectors.

THREATS AND VULNERABILITIES

Our vulnerabilities are increasing steadily, and the means to exploit those weaknesses are readily available. The costs associated with an effective attack continue to drop. The basic attack tools of the cyber-terrorist are a computer, modem, telephone, and user-friendly hacker software.

Cyber-terrorist attacks can take the form of:

- Denial or disruption of computer, cable, satellite, or telecommunications services.
- Monitoring of computer, cable, satellite, or telecommunications systems.
- Disclosure of proprietary, private, or classified information stored within or communicated through computer, cable, and satellite or telecommunications systems.
- Modification or destruction of computer programming codes, computer network databases, stored information, or computer capabilities.
- Manipulation of computer, cable, satellite, or telecommunications services resulting in fraud, financial loss or other federal criminal violation.
- Threats to destroy data or program files.

The ultimate threat to computer security is the insider. These individuals may be disgruntled employees, or represent some group or country. Thus, security clearance checks should be required. Common examples of computer-related employee sabotage include:

- Entering data incorrectly.
- Changing data.
- Deleting data.
- Destroying data or programs with logic bombs. [Logic bomb - A program routine that destroys data; for example, it may reformat the hard disk or randomly insert garbage into data files. A logic bomb may be brought into a personal computer by downloading

a public-domain program that has been tampered with. Once executed, it does its damage right away, whereas a virus keeps on destroying.

"Crashing" systems.

Holding data hostage.

Destroying hardware or facilities.

The Internet is a source for numerous varieties of hacker software, some of which are issued in the guise of network administrator tools, freely available for downloading. Some of these "tools" can be surreptitiously attached to innocent-sounding files and, upon execution, embed themselves in your computer system. These innocent programs can be games, utilities, applications, etc. Although some of these tools have legitimate purposes, people with malicious intent can also use these programs for their own goals.

Financial institutions need to be aware of the indirect threats from groups or countries against our infrastructure, and ensure that these threats are taken into account when developing and testing disaster recovery/contingency plans.

CONTROLS

Technology risk can range from a minor defalcation perpetrated via a computer (internal or external), to major theft, the complete destruction of a bank's records, or the inability of a bank to process data due to some catastrophe such as a power outage. To address external attacks on a computer it is imperative for banks to install a strong intrusion detection system. Such a system must be capable of detecting and recording attempts to break into the bank's computer system, with established procedures for handling such attempts.

A good intrusion detection system must itself be resistant to outside attacks. It must identify and report on deviations from normal processing. And it must be difficult to deceive. No matter how good such a system is, it ultimately will rely on human review of reported activities. It is necessary for such reviews to be part of the normal operating procedure of the bank. Successful intrusion attempts will often be preceded by unsuccessful attempts that the system should be capable of capturing for analysis.

Infrastructure attacks, or infrastructure problems, can be disruptive to a bank's ability to conduct business. Banks may be forced to implement disaster recovery plans based on attacks that have occurred at non-bank locations. Updated, regularly tested disaster recovery plans can minimize the impact of infrastructure attacks.

Additional procedures that banks may implement to avoid becoming a cyber attack victim include:

Maintain adequate expertise to administer, secure, and monitor network security.

Carefully plan network design and architecture in terms of connectivity, placement of key components, and firewalls.

Implement a physical security program that controls and limits the access to computing and information resources to only those who absolutely require such access.

Incorporate logical access controls to computing and information resources that include a program for issuing user IDs, password requirements, anti-virus programs, and monitoring.

Use a log-in banner to ensure that unauthorized users are warned that they may be subject to monitoring.

Report significant unauthorized access attempts to the FBI Computer Crimes unit and the Suspicious Activity Reporting System.

Ensure regular use of virus detection software.

Monitor employee Internet usage; have policies and guidelines regarding usage.

Identify and implement controls over dial-in modems that gain access to internal networks.

Stay abreast of CERT [CERT - Computer Emergency Response Team. Located at Carnegie Mellon University, this incident response team offers advisories that contain enormous amounts of useful, specific security information.] advisories.

Turn audit trails on.

Request trap and tracing [Trap and trace - Trap and trace means using a device that captures the incoming electronic or other impulses which identify the originating phone number of an instrument or device from which a wire or electronic communication was transmitted.] from your local telephone company.

Install caller identification.

Make backups of damaged or altered files.

Maintain old backups to show the status of the original.

Encrypt files.

Encrypt transmissions.

Use one-time password generators.

Use secure firewalls. [Firewall - A system or combination of hardware and software solutions that enforces a boundary between two or more networks.]

Conduct regular background checks of employees in sensitive

positions.

Communicate with peers about best practices to protect against identified threats.

SUMMARY

Ultimately, the best defense against most external cyber attacks is the combination of regular monitoring of network activity, a well-configured firewall, and regular reminders of bank security policies. Installing or running programs received from an unknown source, or from a source that may have accepted it incautiously, risks malicious damage. Controls should be in place at all times.

Contingency/disaster recovery plans should focus on indirect infrastructure threats as well as the direct attacks against the computer systems and underlying data.

Any intrusion, attempted intrusion, or suspicious activity should be immediately reported to a central source (compliance officer, auditor, etc.) for disposition regarding the action the bank should take, and whether a Suspicious Activity Report should be filed.

How your bank addresses the concerns and issues discussed here should be reviewed with your portfolio manager at the next regularly scheduled examination.

Please share this issuance with your data processing/network service providers.

REFERENCES

Detailed information regarding policies, controls and countermeasures can be found in the following documents, each of which is available on the Internet.

OCC Advisory Letter 97-9, November 19, 1997
"Reporting Computer Related Crimes,"
(available at http://www.occ.treas.gov/ftp/advisory/97-9.txt);

OCC Bulletin 98-3, February 4, 1998
"Technology Risk Management,"
(available at http://www.occ.treas.gov/ftp/bulletin/98-3.txt);

OCC Bulletin 98-38, August 24, 1998
"Technology Risk Management: PC Banking,"
(available at http://www.occ.treas.gov/ftp/bulletin/98-38.txt);

FRB SR 97-32 (SUP), December 4, 1997
"Sound Practices Guidance for Information Security for Networks,"
(available at
http://www.bog.frb.fed.us/boarddocs/srletters/1997/SR9732.HTM);

Presidential Decision Directive 63, May 22, 1998

"Protecting America's Critical Infrastructures,"
(available at http://www.ciao.gov/63factsheet.html); and,

18 U. S. C. 1030, Fraud and Related Activity in Connection with Computers,
(available at http://www.usdoj.gov/criminal/cybercrime/1030_new.html).

RESPONSIBLE OFFICE

Questions regarding this banking issuance or the information it contains should be directed to Clifford A. Wilke, director, Bank Technology Division, (202) 874-5920 or via e-mail: clifford.wilke@occ.treas.gov.

Clifford A. Wilke
Director
Bank Technology Division