OCC BULLETIN

Comptroller of the Currency
Administrator of National Banks

Subject: Infrastructure Threats -- Intrusion Risks

Description: Message to Bankers and Examiners

To: Chief Executive Officers of National Banks, Federal Branches and Agencies, Service Providers, Software Vendors, Department and Division Heads, and Examining Personnel.

PURPOSE AND SUMMARY

This bulletin provides guidance to financial institutions on how to prevent, detect, and respond to intrusions into bank computer systems. Intrusions can originate either inside or outside of the bank and can result in a range of damaging outcomes, including the theft of confidential information, unauthorized transfer of funds, and damage to an institution's reputation.

The prevalence and risk of computer intrusions are increasing as information systems become more connected and interdependent and as banks make greater use of Internet banking services and other remote access devices. Recent e-mail-based computer viruses and the distributed denial of service attacks earlier this year revealed that the security of all Internet-connected networks are increasingly intertwined. The number of reported incidences of intrusions nearly tripled from 1998 to 1999, according to Carnegie Mellon University's CERT/CC.[1]

Management can reduce a bank's risk exposure by adopting and regularly reviewing its risk assessment plan, risk mitigation controls, intrusion response policies and procedures, and testing processes. This bulletin provides guidance in each of these critical areas and also highlights information-sharing mechanisms banks can use to keep abreast of current attack techniques and potential vulnerabilities. It supplements OCC Bulletin 99-9, "Infrastructure Threats from Cyber-Terrorists" (March 5, 1999), and other security-related OCC guidance listed in the reference section.

CONTENTS

1 Carnegie Mellon's CERT/CC is part of a federally funded research and development center that helps organizations identify and recover from intrusions. It provides up-to-date information on vulnerabilities, specific attack techniques, and procedures for responding to these attacks.

Comptroller of the Currency
Administrator of National Banks

Subject: Infrastructure Threats -- Intrusion Risks Description: Message to Bankers and Examiners

SECURITY STRATEGIES AND PLANS

Senior management and the board of directors are responsible for overseeing the development and implementation of their bank's security strategy and plan. Key elements to be included in those strategies and plans are an intrusion risk assessment plan, risk mitigation controls, intrusion response policies and procedures, and testing processes. These elements are needed for both internal and outsourced network management and operations and are consistent with the technology risk management process outlined in OCC Bulletin 98-3, "Technology Risk Management" (February 4, 1998); OCC Bulletin 98-38, Technology Risk Management: PC Banking (August 24, 1998); and the "Internet Banking" booklet of the *Comptroller's Handbook* (October 1999).

Intrusion Risk Assessment Plan

The first step in managing the risks of intrusions is to assess the effects that intrusions could have on the institution. Effects may include direct dollar loss, damaged reputation, improper disclosure, lawsuits, or regulatory sanctions. In assessing the risks, management should gather information from multiple sources, including (1) the value and sensitivity of the data and processes to be protected, (2) current and planned protection strategies, (3) potential threats, and (4) the vulnerabilities present in the network environment.[2] Once information is collected,

2 The network environment should be interpreted broadly, including but not limited to internal and external connectivity, hardware and software and their configuration, contractors and employees involved in the operation of the network, and the current means used to mitigate risks.

management should identify threats and the likelihood of those threats materializing, rank critical information assets and operations, and estimate potential damage.

The analysis should be used to develop an intrusion protection strategy and risk management plan. The intrusion protection strategy and risk management plan should be consistent with the bank's information security objectives. It also should balance the cost of implementing adequate security controls with the bank's risk tolerance and profile. The plan should be implemented within a reasonable time. Management should document this information, its analysis of the information, and decisions in forming the protection strategy and risk management plan. By documenting this information, management can better control the assessment process and facilitate future risk assessments.

Management should re-evaluate the strategy and plan when changes are made that could affect the potential for loss, when new vulnerabilities are uncovered, and when the nature and extent of threats change significantly. Changes to network security identified through assessments or other evaluations should be implemented promptly.

Controls to Prevent and Detect Intrusions

Management should determine the controls necessary to deter, detect, and respond to intrusions, consistent with the best practices of information system operators. Controls may include the following:

> **Authentication.** Authentication provides identification by means of some previously agreed upon method, such as passwords and biometrics.[3] The means and strength of authentication should be commensurate with the risk. For instance, passwords should be of an appropriate length, character set, and lifespan[4] for the systems being protected. Employees should be trained to recognize and respond to fraudulent attempts to compromise the integrity of security systems. This may include "social engineering" whereby intruders pose as authorized users to gain access to bank systems or customer records.

3 A method of identifying a person's identity by analyzing a unique physical attribute.
4 The lifespan of a password is the length of time the password allows access to the system. Generally speaking, shorter lifespans reduce the risk of password compromises.

Install and Update Systems. When a bank acquires and installs new or upgraded systems or equipment, it should review security parameters and settings to ensure that these are consistent with the intrusion risk assessment plan. For example, the bank should review user passwords and authorization levels for maintaining "separation of duties" and "need to know" policies. Once installed, security flaws to software and hardware should be identified and remediated through updates or "patches." Continuous monitoring and updating is essential to protect the bank from vulnerabilities. Information related to vulnerabilities and patches are typically available from the vendor, security-related web sites, and in bi-weekly National Infrastructure Protection Center's *CyberNotes.*[5]

Software Integrity. Copies of software and integrity checkers[6] are used to identify unauthorized changes to software. Banks should ensure the security of the integrity checklist and checking software. Where sufficient risk exists, the checklist and software should be stored away from the network, in a location where access is limited. Banks should also protect against viruses and other malicious software by using automated virus scanning software and frequently updating the signature file[7] to enable identification of new viruses.

Attack Profile. Frequently systems are installed with more available components and services than are required for the performance of necessary functions. Banks maintaining unused features may unwittingly enable network penetration by increasing the potential vulnerabilities. To reduce the risk of intrusion, institutions should use the minimum number of system components and services to perform the necessary functions.

Modem Sweep. While access to a system is typically directed through a firewall, sometimes modems are attached to the system directly, perhaps without the knowledge of personnel responsible for security. Those modems can provide an uncontrolled and unmonitored area for attack. Modems that present such vulnerabilities should be identified and either eliminated, or monitored and controlled.

5 Available at http://www.fbi.gov/nipc/cybernotes.htm
6 An integrity checker uses logical analysis to identify whether a file has been changed.
7 The signature file contains the information necessary to identify each virus.

Intrusion Identification. Real-time identification of an attack is essential to minimize damage. Therefore, management should consider the use of real-time intrusion detection software. Generally, this software inspects for patterns or "signatures" that represent known intrusion techniques or unusual system activities. It may not be effective against new attack methods or modified attack patterns. The quality of the software and sophistication of an attack also may reduce the software's effectiveness. To identify intrusions that escape software detection, other practices may be necessary. For example, banks can perform visual examinations and observations of systems and logs for unexpected or unusual activities and behaviors as well as manual examinations of hardware. Since intrusion detection software itself is subject to compromise, banks should take steps to ensure the integrity of the software before it is used.

Firewalls. Firewalls are an important component of network security and can be effective in reducing the risk of a successful attack. The effectiveness of a firewall, however, is dependent on its design and implementation. Because misconfigurations, operating flaws, and the means of attack may render firewalls ineffective, management should consider additional security behind the firewall, such as intrusion identification and encryption.

Encryption. Encryption is a means of securing data. Data can by encrypted when it is transmitted, and when it is stored. Because networks are not impervious to penetration, management should evaluate the need to secure their data as well as their network. Management's use of encryption should be based on an internal risk assessment and a classification of data. The strength of encryption should be proportional to the risk and impact if the data were revealed.

Employee and Contractor Background Checks. Management should ensure that information technology staff, contractors, and others who can make changes to information systems have passed background checks. Management also should revalidate periodically access lists and logon IDs.

Accurate and Complete Records of Uses and Activities. Accurate and complete records of users and activities are essential for analysis, recovery, and development of additional security measures, as well as possible legal action. Information of primary importance includes the methods used to gain access, the extent of the intruder's access to

systems and data, and the intruder's past and current activities. To ensure that adequate records exist, management should consider collecting information about users and user activities, systems, networks, file systems, and applications. Consideration should be given to protecting and securing this information by locating it in a physical location separate from the devices generating the records, writing the data to a tamperproof device, and encrypting the information both in transit and in storage. The OCC expects banks to limit the use of personally identifiable information collected in this manner for security purposes, and to otherwise comply with applicable law and regulations regarding the privacy of personally identifiable information.

Vendor Management. Banks rely on service providers, software vendors, and consultants to manage networks and operations. In outsourcing situations, management should ensure that contractual agreements are comprehensive and clear with regard to the vendor's responsibility for network security, including its monitoring and reporting obligations. Management should monitor the vendor's performance under the contract, as well as assess the vendor's financial condition at least annually.

Intrusion Response Policies and Procedures

Management should establish, document, and review the policies and procedures that guide the bank's response to information system intrusions. The review should take place at least annually, with more frequent reviews if the risk exposure warrants them. The OCC will assess the adequacy of policies and procedures that address the bank's handling of network intrusions in the context of the risks faced by the bank.

Policies and procedures should address the following:

- The priority and sequence of actions to respond to an intrusion. Actions should address the containment and elimination of an intrusion and system restoration. Among other issues, containment actions include a determination of which business processes must remain operational, which systems may be disconnected as a precaution, and how to address authentication compromises (*e.g.,* revealed passwords) across multiple systems.

- Gathering and retaining intrusion information, as discussed below.

- The employee's authority to act, whether by request or by pre-approval, and the process for escalating the intrusion response to progressively higher degrees of intensity and senior management involvement.

- Availability of necessary resources to respond to intrusions. Management should ensure that contact information is available for those that are responsible for responding to intrusions.

- System restoration tools and techniques, including the elimination of the intruder's means of entry and back doors, and the restoration of data and systems to the pre-intrusion state.

- Notification and reporting to operators of other affected systems, users, regulators, incident response organizations, and law enforcement. Guidelines for filing a Suspicious Activity Report for suspected computer related crimes are discussed below, and in OCC Advisory Letter 97-9, "Reporting Computer Related Crimes" (November 19, 1997).

- Periodic testing, as discussed below.

- Staff training resources and requirements.

Gathering and Retaining Intrusion Information. Particular care should be taken when gathering intrusion information. The OCC expects management to clearly assess the tradeoff between enabling an easier recovery by gathering information about an intruder and the risk that an intruder will inflict additional damage while that information is being gathered. Management should establish and communicate procedures and guidelines to employees through policies, procedures, and training. Intrusion evidence should be maintained in a fashion that enables recovery while facilitating subsequent actions by law enforcement. Legal chain of custody requirements must be considered. In general, legal chain of custody requirements address controlling and securing evidence from the time of the intrusion until it is turned over to law enforcement personnel. Chain of custody actions, and those actions that should be guarded against, should be identified and embodied in the bank's policies, procedures, and training.

Suspicious Activity Reporting. National banks are required to report intrusions and other

computer crimes to the OCC and law enforcement by filing a Suspicious Activity Report (SAR) form and submitting it to the Financial Crimes Enforcement Network (FinCEN), in accordance with 12 USC 21.11. This reporting obligation exists regardless of whether the institution has reported the intrusion to the information-sharing organizations discussed below. For purposes of the regulation and the SAR form instructions, an "intrusion" is defined as gaining access to the computer system of a financial institution to remove, steal, procure or otherwise affect information or funds of the institution or customers. It also includes actions that damage, disable, or otherwise affect critical systems of the institution. For example, distributed denial of service attaches (DDoS) attacks should be reported on a SAR because they may temporarily disable critical systems of financial institutions.

Testing. Management should ensure that information system networks are tested regularly. The nature, extent, and frequency of tests should be proportionate to the risks of intrusions from external and internal sources.[8] Management should select qualified and reputable individuals to perform the tests and ensure that tests do not inadvertently damage information systems or reveal confidential information to unauthorized individuals. Management should oversee the tests, review test results, and respond to deficiencies in a timely manner.

INFORMATION SHARING

Information sharing among reliable and reputable experts can help institutions reduce the risk of information system intrusions. The OCC encourages management to participate in information-sharing mechanisms as part of an effort to detect and respond to intrusions and vulnerabilities. Mechanisms for information sharing are being developed by many different organizations, each with a different mission and operation. In addition, many vendors offer information sharing and analysis services. Three organizations that are primarily involved with the federal government's national information security initiatives are the Financial Services Information Sharing and Analysis Center (FS/ISAC), the Federal Bureau of Investigation (FBI), and Carnegie Mellon University's CERT/CC.

The FS/ISAC was formed in response to Presidential Decision Directive 63: Critical

8 In accordance with OCC Bulletin 98-38, "Technology Risk Management: PC Banking" (August 24, 1998), management should ensure that an objective, qualified source conducts a penetration test of Internet banking systems at least once a year or more frequently when appropriate.

Comptroller of the Currency
Administrator of National Banks

Subject: Infrastructure Threats -- Intrusion Risks

Description: Message to Bankers and Examiners

Infrastructure Protection (May 22, 1998), which encourages the banking, finance, and other industries to establish information-sharing efforts in conjunction with the federal government. The FS/ISAC allows financial services entities to report incidents anonymously. In turn, the FS/ISAC rapidly distributes information about attacks to the FS/ISAC members. Banks can contact FS/ISAC by telephone at (888) 660-0134, e-mail at admin@fsisac.com or their Web site at http://www.fsisac.com.

The FBI operates the National Information Protection Center Infraguard outreach effort. Since Infraguard supports law enforcement efforts, Infraguard members submit two versions of an incident report. One complete version is used by law enforcement and contains information that identifies the reporting member. The other version does not contain that identifying information, and is distributed to other Infraguard members. Banks can contact the FBI by contacting local FBI field offices or via e-mail at nipc@fbi.gov.

CERT/CC is part of a federally funded research and development center at Carnegie Mellon University that helps organizations identify vulnerabilities and recover from intrusions. It provides up-to-date information on specific attacks (including viruses and denial of service) and collates and shares information with other organizations. CERT/CC does not require membership to report problems. Banks can contact CERT/CC by phone at (412) 268-7090 or e-mail at cert@cert.org.

RESPONSIBLE OFFICE

Questions regarding this banking issuance 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

Appendix

Appendix -- References

The OCC issued Bulletin 99-9 (March 5, 1999) to identify and raise awareness of the threats and vulnerabilities created by cyber-terrorism to the financial services industry. It focused on a national bank's ability to protect the integrity, confidentiality, and availability of information technology resources. This document supplements Bulletin 99-9 and relevant parts of OCC Bulletin 98-38, Technology Risk Management: PC Banking (August 24, 1998). It also supplements OCC Bulletin 98-3, Technology Risk Management (February 4, 1998), which describes the application of the OCC's supervision by risk framework to the risks posed by technology. The objectives and procedures that examiners use to evaluate the quality of risk management and quantity of risk are addressed in the OCC's "Internet Banking" booklet(October 1999).

The FFIEC recently issued an Information Security Precautions Advisory (as transmitted by OCC Advisory Letter 99-12 on November 22, 1999). That advisory addressed the potential for information system intrusions during the Year 2000 rollover.

For additional information on information security policies and controls see the following documents.

- Comptroller's Handbook -- Internet Banking, October 1999
- OCC Alert 2000-1, February 11, 2000 - "Internet Security: Distributed Denial of Service Attacks" (available at http://www.occ.treas.gov/ftp/alert/2000-1.doc)
- OCC Bulletin 99-9, March 5, 1999 - "Infrastructure Threats from Cyber-Terrorists," (available at http://www.occ.treas.gov/ftp/bulletin/99-9.txt)
- 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)
- OCC Banking Circular 229, May 31, 1988 - "Information Security"
- FFIEC AL 99-12, November 19, 1999 - "Information Security Precautions Advisory" (available at http://www.occ.treas.gov/ftp/advisory/99-12.txt)

- FFIEC IS Examination Handbook (1996)
- FRB SR 97-32 (SUP), December 4, 1997 – "Sound Practices Guidance for Information Security for Networks"
- FDIC FIL 99-68, July 17, 1999 -- "Risk Assessment Tools and Practices for Information System Security" (available at http://192.147.69.45/news/news/financial/1999/FIL9968a.HTML)
- Presidential Decision Directive 63, May 22, 1998 – "Protecting America's Critical Infrastructures," (available at http://www.info-sec.com/ciao/63factsheet.html);
- 18 USC 1030, Fraud and Related Activity in Connection with Computers," (available at http://www.usdoj.gov/criminal/cybercrime/1030_new.html)
- General Accounting Office "Information Risk Assessment: Practices of Leading Organizations", November 1999 (available at http://www.gao.gov/AIndexFY99/abstracts/ai99139.htm)
- Carnegie Mellon Software Engineering Institute Security Improvement Module CMU/SEI-SIM-004, "Securing Desktop Workstations," February 1999 (available at http://www.cert.org/security-improvement/modules/m04.html)
- Carnegie Mellon Software Engineering Institute Security Improvement Module CMU-SIM-007, "Securing Network Servers," February 1999, (available at http://www.cert.org/security-improvement/modules/m07.html)
- Carnegie Mellon Software Engineering Institute Security Improvement Module CMU-SIM-005, "Preparing to Detect Signs of Intrusion," June 1998 (available at http://www.cert.org/security-improvement/modules/m05.html)
- Carnegie Mellon Software Engineering Institute Security Improvement Module CMU-SIM-001, "Detecting Signs of Intrusion," August 1997 (available at http://www.cert.org/security-improvement/modules/m01.html)
- Carnegie Mellon Software Engineering Institute Security Improvement Module CMU-SIM-006, "Responding to Intrusions", February 1999 (available at http://www.cert.org/security-improvement/modules/m06.html)
- Carnegie Mellon Software Engineering Institute Technical Report CMU/SEI-99-TR-028 "State of the Practice of Intrusion Detection Technologies," February 2000, (available at http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028abstract.html)
- Financial Services Information Sharing and Analysis Center (available at http://www.fsisac.com)

- Infraguard Outreach Effort (available at http://www.fbi.gov/nipc/outreachinfragd.htm)
- CERT/CC (available at http://www.cert.org).