RB-2000-02 Guidance on Information System Security

BACKGROUND

The purpose of this Bulletin is to provide credit unions with background information and guidance on various risk assessment tools and practices related to information security. Credit unions using the Internet or other computer networks are exposed to various categories of risk that could result in the possibility of financial loss and reputational harm. Given the rapid growth of the Internet and networking technology, the available risk assessment tools and practices are becoming more important for information security.

This Bulletin provides a summary of critical points, discusses components of a sound information security program, and describes the risk assessment and risk management processes for information security. The appendix provides specific information on certain risk assessment tools and practices that may be part of a credit union's information security program. The Bulletin and appendix are intended to provide useful information and guidance, and not to create new examination standards, impose new regulatory requirements, or represent an exclusive description of the various ways credit unions can implement effective information security programs.

Whether credit unions contract with third-party providers for computer services or maintain computer services in-house, credit union management is responsible for ensuring that systems and data are protected against risks associated with emerging technologies and computer networks. If a credit union is relying on a third-party provider, management must generally understand the provider's information security program to effectively evaluate the security system's ability

to protect credit union and member data.

The Department has previously issued guidance on information security concerns. This Bulletin is designed to supplement Regulatory Bulletin 1999-01, “Guidance on Electronic Financial Services,” dated September 1, 1999, and to complement the Department’s soon-to-be implemented electronic commerce examination procedures.

SUMMARY OF CRITICAL POINTS

To ensure the security of information systems and data, credit unions should have a sound information security program that identifies, measures, monitors, and manages potential risk exposure. Fundamental to an effective information security program is an ongoing risk assessment of threats and vulnerabilities surrounding networked and/or Internet systems. Credit unions should consider the various measures available to support and enhance information security programs. The appendix to this Bulletin describes certain vulnerability assessment tools and intrusion detection methods that can be useful in preventing and identifying attempted external break-ins or internal misuse of information systems. Credit unions should also consider plans for responding to an information security incident.

INFORMATION SECURITY PROGRAM

A credit union’s board of directors and senior management should be aware of information security issues and be involved in developing an appropriate information security program. A comprehensive information security policy should outline a proactive and ongoing program incorporating three components:

- Prevention
- Detection
- Response

Prevention measures include sound security policies, well-designed system architecture, properly configured firewalls, and strong authentication programs. This Bulletin discusses two additional prevention measures: vulnerability assessment tools and penetration analyses. Vulnerability assessment tools generally involve running scans on a system to proactively detect known vulnerabilities such as security flaws and bugs in software and hardware. These tools can also detect holes allowing unauthorized access to a network or insiders to misuse the system. Penetration analysis involves an independent party (internal or external) testing a credit union's information system security to identify (and possibly exploit) vulnerabilities in the system and surrounding processes. Using vulnerability assessment tools and performing regular penetration analyses will assist a credit union in determining what security weaknesses exist in its information systems.

Detection measures involve analyzing available information to determine if an information system has been compromised, misused, or accessed by unauthorized individuals. Detection measures may be enhanced by the use of intrusion detection systems (IDSs) that act as a burglar alarm, alerting the credit union or service provider to potential external break-ins or internal misuse of the system(s) being monitored.

Another key area involves preparing a *response* program to handle suspected intrusions and system misuse once they are detected. Credit unions should have an effective incident response program outlined in a security policy that prioritizes incidents, discusses appropriate responses to incidents, and establishes reporting requirements.

The appendix provides a detailed discussion on prevention (vulnerability assessment tools and penetration analyses), detection (IDSs tools), and response measures. Before implementing some or all of these measures, a credit union should perform an information security risk assessment.

Depending on the risk assessment, certain risk assessment tools and practices discussed in this Bulletin may be appropriate. However, use of these measures should not result in decreased emphasis on information security or the need for human expertise.

RISK ASSESSMENT/MANAGEMENT

A thorough and proactive risk assessment is the first step in establishing a sound security program. This is the ongoing process of evaluating threats and vulnerabilities, and establishing an appropriate risk management program to mitigate potential monetary losses and harm to a credit union's reputation. Threats have the potential to harm a credit union, while vulnerabilities are weaknesses that can be exploited.

The extent of the information security program should be commensurate with the degree of risk associated with the credit union's systems, networks, and information assets. For example, compared to an information-only Web site, credit unions offering transactional electronic activities are exposed to greater risks. Further, real-time funds transfers generally pose greater risks than delayed or batch-processed transactions because the items are processed immediately. The extent to which a credit union contracts with third-party vendors will also affect the nature of the risk assessment program.

Performing the Risk Assessment and Determining Vulnerabilities

Performing a sound risk assessment is critical to establishing an effective information security program. The risk assessment provides a framework for establishing policy guidelines and identifying the risk assessment tools and practices that may be appropriate for a credit union. Credit

unions should have a written information security policy, sound security policy guidelines, and well-designed system architecture, as well as provide for physical security, employee education, and testing as part of an effective program.

When credit unions contract with third-party providers for information system services, they should have a sound oversight program. At a minimum, the security-related clauses of a written contract should define the responsibilities of both parties with respect to data confidentiality, system security, and notification procedures in the event of data or system compromise. The credit union needs to conduct a sufficient analysis of the provider's security program, including how the provider uses available risk assessment tools and practices. Credit unions also should obtain copies of independent penetration tests run against the provider's system.

When assessing information security products, management should be aware that many products offer a combination of risk assessment features and can cover single or multiple operating systems. Several organizations provide independent assessment and certifications of the adequacy of computer security products (e.g., firewalls). While the underlying product may be certified, credit unions should realize that the manner in which the products are configured and ultimately used is an integral part of the products' effectiveness. If relying on the certification, credit unions should understand the certification process used by the organization certifying the security product. Other examples of items to consider in the risk assessment process include:

- *Identifying mission-critical information systems and determining the effectiveness of current information security programs.* For example, vulnerability might involve critical systems that are not reasonably isolated from the Internet and

external access via modem. Having up-to-date inventory listings of hardware and software, as well as system topologies, is important in this process.

- *Assessing the importance and sensitivity of information, and the likelihood of outside break-ins (e.g., by hackers) and insider misuse of information.* For example, if a member depositor list were made public, that disclosure could expose the credit union to reputational risk and the potential loss of deposits. Further, the credit union could be harmed if human resource data (e.g., salaries and personnel files) were made public. The assessment should identify systems that allow the transfer of funds, other assets, or sensitive data/confidential information, and review the appropriateness of access controls and other security policy settings.
- *Assessing the risks posed by electronic connections with business partners.* The other entity may have poor access controls that could potentially lead to an indirect compromise of the credit union's system. Another example involves vendors that may be allowed to access the credit union's system without proper security safeguards, such as firewalls. This could result in open access to critical information that the vendor may have "no need to know."
- *Determining legal implications and contingent liability concerns associated with any of the above.*For example, if hackers successfully access a credit union's system and use it to subsequently attack others, the credit union may be liable for damages incurred by the party that is attacked.

Potential Threats to Consider

Serious hackers, interested computer novices, dishonest vendors or competitors, disgruntled current or former employees, organized crime, or even agents of espionage pose a potential threat to a credit union's computer security. The Internet provides a wealth of information to credit unions and hackers alike on known security flaws in hardware and software. Using almost any search engine, average Internet users can quickly find information describing how to break into various systems by exploiting known security flaws and software bugs. Hackers also may breach security by misusing vulnerability assessment tools to probe network systems, then exploiting any identified weaknesses to gain unauthorized access to a system. Internal misuse of information systems remains an ever-present security threat.

Many break-ins or insider misuses of information occur due to poor security programs. Hackers often exploit well-known weaknesses and security defects in operating systems that have not been appropriately addressed by the credit union. Inadequate maintenance and improper system design may also allow hackers to exploit a security system. New security risks arise from evolving attack methods or newly detected holes and bugs in existing software and hardware. Also, new risks may be introduced as systems are altered or upgraded, or through the improper setup of available security-related tools. A credit union needs to stay abreast of new security threats and vulnerabilities. It is equally important to keep up to date on the latest security patches and version upgrades that are available to fix security flaws and bugs. Information security and relevant vendor Web sites contain much of this information.

Systems can be vulnerable to a variety of threats, including the misuse or theft of passwords. Hackers may use password-cracking programs to figure out poorly selected passwords.

The passwords may then be used to access other parts of the system. By monitoring network traffic, unauthorized users can easily steal unencrypted passwords. The theft of passwords is more difficult if they are encrypted. Employees or hackers may also attempt to compromise system administrator access (root access), tamper with critical files, read confidential e-mail, or initiate unauthorized e-mails or transactions.

Hackers may use "social engineering," a scheme using social techniques to obtain technical information required to access a system. A hacker may claim to be someone authorized to access the system such as an employee or a certain vendor or contractor. The hacker may then attempt to get a real employee to reveal user names or passwords, or even set up new computer accounts. Another threat involves the practice of "war dialing," in which hackers use a program that automatically dials telephone numbers and searches for modem lines that bypass network firewalls and other security measures. A few other common forms of system attack include:

- *Denial of service (system failure),* which is any action preventing a system from operating as intended. It may be the unauthorized destruction, modification, or delay of service. For example, in a "SYN Flood" attack, a system can be flooded with requests to establish a connection, leaving the system with more open connections than it can support. Then, legitimate users of the system being attacked are not allowed to connect until the open connections are closed or can time out.
- *Internet Protocol (IP) spoofing,* which allows an intruder via the Internet to effectively impersonate a local system's IP address in an attempt to gain access to that system. If other local systems perform

session authentication based on a connection's IP address, those systems may misinterpret incoming connections from the intruder as originating from a local trusted host and not require a password.

- *Trojan horses,* which are programs that contain additional (hidden) functions that usually allow malicious or unintended activities. A Trojan horse program generally performs unintended functions that may include replacing programs, or collecting, falsifying, or destroying data. Trojan horses can be attached to e-mails and may create a "back door" that allows unrestricted access to a system. The programs may automatically exclude logging and other information that would allow the intruder to be traced.
- *Viruses,* which are computer programs that may be embedded in other code and can self-replicate. Once active, they may take unwanted and unexpected actions that can result in either nondestructive or destructive outcomes in the host computer programs. The virus program may also move into multiple platforms, date files, or devices on a system and spread through multiple systems in a network. Virus programs may be contained in an e-mail attachment and become active when the attachment is opened.

CONCLUSION

It is important for credit unions to develop and implement appropriate information security programs. Whether systems are maintained in-house or by third-party vendors, appropriate

security controls and risk management techniques must be employed. A security program includes effective security policies and system architecture, which may be supported by the risk assessment tools and practices discussed in the Bulletin and appendix. Information security threats and vulnerabilities, as well as their countermeasures, will continue to evolve. As such, credit unions should have a proactive risk assessment process that identifies emerging threats and vulnerabilities to information systems.

A sound information security policy identifies prevention, detection, and response measures. The appendix provides more details on risk assessment tools and practices that may be used to improve information security programs. Preventive measures may include regularly using vulnerability assessment tools and conducting periodic penetration analyses. Intrusion detection tools can be effective in detecting potential intrusion or system misuse. Credit unions should also develop a response program to effectively handle any information security breaches that may occur.