Risk Assessment Tools And Practices For Information System Security

FIL-68-99
July 7, 1999

TO: CHIEF EXECUTIVE OFFICER
SUBJECT: *FDIC Issues Paper on Information System Security Issues*

The Federal Deposit Insurance Corporation (FDIC) is providing financial institutions the attached paper on information system security issues entitled "Risk Assessment Tools and Practices for Information System Security." Bank management is responsible for ensuring that systems and data are protected against risks associated with emerging technology and computer networks.

An ever-increasing number of financial institutions are using the Internet or other computer networks as an information resource or delivery channel. In 1997, the FDIC instituted safety and soundness electronic banking examination procedures, and provided guidance on security risks associated with the Internet. Information security issues continue to arise, and information gathered through the FDIC's electronic banking examination process indicates the need for additional guidance on information system security issues.

The attached paper emphasizes three primary components of a sound information security program: prevention, detection, and response. The extent of an institution's information security program will depend on the nature of its activities and should be based on a comprehensive risk assessment. A variety of tools are described in the paper that can facilitate the risk assessment process. The guidance does not specifically recommend which tools and practices an institution should use. These will depend on each institution's risk assessment, including the identification of potential threats to and vulnerabilities of its information systems. The guidance is intended to provide useful information to financial institutions, not to create new examination standards, impose new regulatory requirements, or recommend a specific course of action.

The issues discussed in the paper are also relevant to institutions that contract with third-party providers for information system services. Institutions that contract for such services should have a sound vendor management program that generally incorporates the items discussed in the guidance.

This guidance is designed to supplement Financial Institution Letter 131-97, "Security Risks Associated With the Internet," issued December 18, 1997, and to complement the FDIC's safety and soundness electronic banking examination procedures. Related guidance can be found in the *FFIEC Information Systems Examination Handbook.*

For more information, please contact your Division of Supervision Regional Office or Examination Specialist Cynthia A. Bonnette at (202) 898-6583.

James L. Sexton
Director

Attachment: Risk Assessment Tools and Practices for Information System Security

Distribution: FDIC-Supervised Banks (Commercial and Savings)

NOTE: Paper copies of FDIC financial institutions letters may be obtained through the FDIC's Public

Information Center, 801 17th Street, NW, Room 100, Washington, DC 20434 (800-276-6003 or 202-416-6940).

RISK ASSESSMENT TOOLS AND PRACTICES FOR INFORMATION SYSTEM SECURITY

INTRODUCTION

The purpose of this paper is to provide financial institutions and examiners with background information and guidance on various risk assessment tools and practices related to information security. Institutions 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 paper 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 an institution's information security program. The paper and appendix are intended to provide useful information and guidance, not to create new examination standards, impose new regulatory requirements, or represent an exclusive description of the various ways financial institutions can implement effective information security programs.

Whether financial institutions contract with third-party providers[1] for computer services such as Internet banking, or maintain computer services in-house, bank management is responsible for ensuring that systems and data are protected against risks associated with emerging technologies and computer networks. If a bank 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 bank and customer data.

The FDIC has previously issued guidance on information security concerns such as data privacy and confidentiality, data integrity, authentication, non-repudiation, and access control/system design. This paper is designed to supplement Financial Institution Letter 131-97, "Security Risks Associated With the Internet," dated December 18, 1997, and to complement the FDIC's safety and soundness electronic banking examination procedures. Related guidance can be found in the *FFIEC Information Systems Examination Handbook.*

[1] For the purposes of this paper, "third-party provider" is broadly defined. Third-party providers include entities that may provide the following services or products to institutions: system design, development, administration, and maintenance services; data processing services; and hardware and/or software solutions.

SUMMARY OF CRITICAL POINTS

To ensure the security of information systems and data, financial institutions should have a sound information security program that identifies, measures, monitors, and manages potential risk exposure. Fundamental to an effective information security program is ongoing risk assessment of threats and vulnerabilities surrounding networked and/or Internet systems. Institutions should consider the various measures available to support and enhance information security programs. The appendix to this paper 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. Institutions should also consider plans for responding to an information security incident.

INFORMATION SECURITY PROGRAM

A financial institution'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 paper 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 an institution'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 an institution 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 bank 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. Institutions 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 (IDS tools), and response measures. Before implementing some or all of these measures, an institution should perform an information security risk assessment. Depending on the risk assessment, certain risk assessment tools and practices discussed in this paper 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 an institution's reputation. Threats have the potential to harm an institution, 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 institution's systems, networks, and information assets. For example, compared to an information-only Web site, institutions offering transactional Internet banking 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 an institution 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 an institution. Banks still 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 institutions 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 institution needs to conduct a sufficient analysis of the provider's security program, including how the provider uses available risk assessment tools and practices. Institutions 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 assessments and certifications of the adequacy of computer security products (e.g., firewalls). While the underlying product may be certified, banks 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, banks 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, a 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 large depositor list were made public, that disclosure could expose the bank to reputational risk and the potential loss of deposits. Further, the institution 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 bank's system. Another example involves vendors that may be allowed to access the bank'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 bank's system and use it to subsequently attack others, the bank 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 an institution's computer security. The Internet provides a wealth of information to banks 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 institution. 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. An institution 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, data 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 financial institutions 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 this guidance paper and appendix. Information security threats and vulnerabilities, as well as their countermeasures, will continue to evolve. As such, institutions 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 intrusions or system misuse. Institutions should also develop a response program to effectively handle any information security breaches that may occur.

APPENDIX

PART ONE – PREVENTION: Discusses the use of vulnerability assessment tools and penetration analyses. When used regularly, both techniques can be integral components of an institution's information security program.

VULNERABILITY ASSESSMENT TOOLS

Vulnerability assessment tools, also called security scanning tools, assess the security of network or host systems and report system vulnerabilities. These tools can scan networks, servers, firewalls, routers, and applications for vulnerabilities. Generally, the tools can detect known security flaws or bugs in software and hardware, determine if the systems are susceptible to known attacks and exploits, and search for system vulnerabilities such as settings contrary to established security policies.

In evaluating a vulnerability assessment tool, management should consider how frequently the tool is updated to include the detection of any new weaknesses such as security flaws and bugs. If there is a time delay before a system patch is made available to correct an identified weakness, mitigating controls may be needed until the system patch is issued.

Generally, vulnerability assessment tools are not run in real-time, but they are commonly run on a periodic basis. When using the tools, it is important to ensure that the results from the scan are secure and only provided to authorized parties. The tools can generate both technical and management reports, including text, charts, and graphs. The vulnerability assessment reports can tell a user what weaknesses exist and how to fix them. Some tools can automatically fix vulnerabilities after detection.

Host- Versus Network-Based Vulnerability Assessment Tools

As in intrusion detection systems, which are discussed later in this appendix, there are generally two types of vulnerability assessment tools: host-based and network-based. Another category is sometimes used for products that assess vulnerabilities of specific applications (application-based) on a host. A host is generally a single computer or workstation that can be connected to a computer network. Host-based tools assess the vulnerabilities of specific hosts. They usually reside on servers, but can be placed on specific desktop computers, routers, or even firewalls. Network-based vulnerability assessment tools generally reside on the network, specifically analyzing the network to determine if it is vulnerable to known attacks. Both host- and network-based products offer valuable features, and the risk assessment process should help an institution determine which is best for its needs. Information systems personnel should understand the types of tools available, how they operate, where they are located, and the output generated from the tools.

Host-based vulnerability assessment tools are effective at identifying security risks that result from internal misuse or hackers using a compromised system. They can detect holes that would allow access to a system such as unauthorized modems, easily guessed passwords, and unchanged vendor default passwords. The tools can detect system vulnerabilities such as poor virus protection capabilities; identify hosts that are configured improperly; and provide basic information such as user log-on hours, password/account expiration settings, and users with dial-in access. The tools may also provide a periodic check to confirm that various security policies are being followed. For instance, they can check user permissions to access files and directories, and identify files and directories without ownership.

Network-based vulnerability assessment tools are more effective than host-based at detecting network attacks such as denial of service and Internet Protocol (IP) spoofing. Network tools can detect unauthorized systems on a network or insecure connections to business partners. Running a host-based scan does not consume network overhead, but can consume processing time and available storage on the host. Conversely, frequently running a network-based scan as part of daily operations increases network traffic during the scan. This may cause inadvertent network problems such as router crashes.

PENETRATION ANALYSIS

After the initial risk assessment is completed, management may determine that a penetration analysis (test) should be conducted. For the purpose of this paper, “penetration analysis” is broadly defined. Bank management should determine the scope and objectives of the analysis. The scope can range from a specific test of a particular information system’s security or a review of multiple information security processes in an institution.

A penetration analysis usually involves a team of experts who identify an information system’s vulnerability to a series of attacks. The evaluators may attempt to circumvent the security features of a system by exploiting the identified vulnerabilities. Similar to running vulnerability scanning tools, the objective of a penetration analysis is to locate system vulnerabilities so that appropriate corrective steps can be taken.

The analysis can apply to any institution with a network, but becomes more important if system access is allowed via an external connection such as the Internet. The analysis should be independent and may be conducted by a trusted third party, qualified internal audit team, or a combination of both. The information security policy should address the frequency and scope of the analysis. In determining the scope of the analysis, items to consider include internal vs. external threats, systems to include in the test, testing methods, and system architectures.

A penetration analysis is a snapshot of the security at a point in time and does not provide a complete guaranty that the system(s) being tested is secure. It can test the effectiveness of security controls and preparedness measures. Depending on the scope of the analysis, the evaluators may work under the same constraints applied to ordinary internal or external users. Conversely, the evaluators may use all system design and implementation documentation. It is common for the evaluators to be given just the IP address of the institution and any other public information, such as a listing of officers that is normally available to outside hackers. The evaluators may use vulnerability assessment tools, and employ some of the attack methods discussed in this paper such as social engineering and war dialing. After completing the agreed-upon analysis, the evaluators should provide the institution a detailed written report. The report should identify vulnerabilities, prioritize weaknesses, and provide recommendations for corrective action.

A penetration analysis itself can introduce new risks to an institution; therefore, several items should be considered before having an analysis completed, including the following:

- *If using outside testers, the reputation of the firm or consultants hired.* The evaluators will assess the weaknesses in the bank's information security system. As such, the confidentiality of results and bank data is crucial. Just like screening potential employees prior to their hire, banks should carefully screen firms, consultants, and subcontractors who are entrusted with access to sensitive data. A bank may want to require security clearance checks on the evaluators. An institution should ask if the evaluators have liability insurance in case something goes wrong during the test. The bank should enter into a written contact with the evaluators, which at a minimum should address the above items.
- *If using internal testers, the independence of the testers from system administrators*.
- *The secrecy of the test.* Some senior executives may order an analysis without the knowledge of information systems personnel. This can create unwanted results, including the notification of law enforcement personnel and wasted resources responding to an attack. To prevent excessive responses to the attacks, bank management may consider informing certain individuals in the organization of the penetration analysis.
- *The importance of the systems to be tested.* Some systems may be too critical to be exposed to some of the methods used by the evaluators such as a critical database that could be damaged during the test.

PART TWO – DETECTION: Discusses intrusion detection systems, and using these tools as the detection component of an institution's information security program.

INTRUSION DETECTION SYSTEMS

Vulnerability assessments and penetration analyses help ensure that appropriate security precautions have been implemented and that system security configurations are appropriate. The next step is to monitor the system for intrusions and unusual activities. Intrusion detection systems (IDSs) may be useful because they act as a burglar alarm, reporting potential intrusions to appropriate personnel. By analyzing the information generated by the systems being guarded, IDSs help determine if necessary safeguards are in place and are protecting the system as intended. In addition, they can be configured to automatically respond to intrusions.

Computer system components or applications can generate detailed, lengthy logs or audit trails that system administrators can manually review for unusual events. IDSs automate the review of logs and audit data, which increases the review's overall efficiency by reducing costs and the time and level of skill necessary to review the logs.

Typically, there are three components to an IDS. First is an agent, which is the component that actually collects the information. Second is a manager, which processes the information collected by the agents. Third is a console, which allows authorized information systems personnel to remotely install and upgrade agents, define intrusion detection scenarios across agents, and track intrusions as they occur. Depending on the complexity of the IDS, there can be multiple agent and manager components.

Generally, IDS products use three different methods to detect intrusions. First, they can look for identified attack signatures, which are streams or patterns of data previously identified as an attack. Second, they can look for system misuse such as unauthorized attempts to access files or disallowed traffic inside the firewall. Third, they can look for activities that are different from the user's or system's normal pattern. These "anomaly-based" products (which use artificial intelligence) are designed to detect subtle changes or new attack patterns, and then notify appropriate personnel that an intrusion may be occurring. Some anomaly-based products are created to update normal use patterns on a regular basis. Poorly designed anomaly-based products can trigger frequent false-positive responses.

Although IDSs may be an integral part of an institution's overall system security, they will not protect a system from previously unknown threats or vulnerabilities. They are not self-sufficient and do not compensate for weak authentication procedures (e.g., when an intruder already knows a password to access the system). Also, IDSs often have overlapping features with other security products, such as firewalls. IDSs provide additional protections by helping to determine if the firewall programs are working properly and by helping to detect internal abuses. Both firewalls and IDSs need to be properly configured and updated to combat new types of attacks. In addition, management should be aware that the state of these products is highly dynamic and IDS capabilities are evolving.

IDS tools can generate both technical and management reports, including text, charts, and graphs. The IDS reports can provide background information on the type of attack and recommend courses of action. When an intrusion is detected, the IDS can automatically begin to collect additional information on the attacker, which may be needed later for documentation purposes.

Host- Versus Network-Based IDS Tools

As with vulnerability assessment tools, there are generally two types of IDS products: host-based and network-based. A third product category is sometimes used for IDSs that look for unusual application events (application-based) on a host. Both network- and host-based tools offer valuable features, and the risk assessment process should help institutions determine if either, or a combination of both, is best for their needs.

Host-Based IDSs

Host-based IDSs are also known as audit trail analysis tools or server-based IDSs (often placed on servers). A host-based IDS will look for potential intrusions or patterns of misuse by monitoring host event activities, audit logs, and other security-related activities. The tools will track audit trails from operating systems, applications, Web servers, routers, and firewalls, as well as monitor critical files for Trojan horses and unauthorized changes. This can provide valuable evidence of a break-in and can assist in assessing damage because the intruder’s actions are logged on the specific hosts. If done in real-time, the IDS can promptly notify the bank of unauthorized attempts to gain system administrator (root) controls, access or change critical files, or replace log-in programs.

An important benefit of host-based IDSs is that they are effective in detecting insider misuse because they monitor activities on the specific hosts. For example, they can monitor a user’s attempt to access a restricted file, or an attempt to execute a system administrator’s command. In addition, they can monitor encrypted transmissions as the data is generally decrypted before it is logged at the host.

A problem with host-based systems is that notification of the attack is delayed if an agent does not examine the audit trail in real-time. This problem relates to the relatively large consumption of computer processing speed and disk space that is required to run these programs in real-time. If not run in real-time, they still allow a bank to identify larger trends and problems with system security.

Network-Based IDSs

With network-based IDSs, software or sniffers are placed on one or multiple points across the network. The sniffer agent analyzes packets of information moving across the network for potential intrusions. Network packets contain data, including the message and headers that identify the sending and receiving parties. Network-based IDSs look for patterns of misuse, specific types of attacks, and unusual activity such as unexpected volume and types of network traffic. Compared to host-based IDSs, certain types of network-orientated attacks such as IP spoofing, packet floods, and denial of service, are best detected through packet examination.

Network-based IDSs can detect potential intrusions in real-time, and offer concurrent notification and response capabilities to potential intrusions. The software does not need to be put on the various hosts throughout the network, thus it is generally easier to monitor and may be less expensive than host-based IDSs.

Network-based IDSs sometimes mistakenly identify normal traffic as an intrusion ("false positives") and vice versa ("false negatives"). They can have difficulties detecting slow attacks and experience problems with busy networks. Network-based IDSs cannot monitor encrypted transmissions (only detect that data is being transferred across the network), and are less effective at detecting insider misuse because network packet analysis does not monitor the activities on specific hosts.

Factors to Consider in Evaluating IDSs

Once it is determined that an IDS is necessary to detect possible security breaches, several factors should be considered in evaluating IDSs, including:

- *The comprehensiveness of the attack signature database, including the frequency of updates that incorporate newly identified concerns.* Most products rely on vendor updates, so banks need to assess the timeliness of the IDS vendor's updates. Products can be updated through Internet downloads, CD-ROM or floppy disk updates, or even manually if the user has a sufficient degree of technical knowledge.
- *The effectiveness of the IDS in protecting an institution from both internal and external threats to a computer system.* The IDS should limit the number of false positives (incorrectly identifying an attack when none has occurred) and false negatives (not identifying an attack when one has occurred).
- *The impact on performance of the network and/or host(s).* Generally, IDSs work on a real-time basis. Real-time analysis provides quicker notification of potential intrusions; however, it can reduce system performance due to the additional memory and processing requirements. Non-real-time analysis generally consumes fewer resources, but has the disadvantage that the potential intrusion has already occurred. Knowledgeable intruders, moreover, can manipulate audit trails, making the after-the-fact analysis useless in detecting these particular intruders.
- *The security of the IDS itself and how secure the update process is, especially if updated remotely.*
- *The reporting and automated response capabilities.* IDSs will sometimes generate more information than can be reviewed by present qualified staff. Also, for privacy

reasons, management should consider informing all affected system users about the scope and type of monitoring being conducted.

Other things to consider include training and support from the vendor, cost of hardware, software, and maintenance agreements, integration with vulnerability assessment tools, and configuration capabilities.

Determining Which is Best for an Institution

An institution's risk assessment process should first determine whether an IDS is necessary. Next, the type or placement of an IDS depends on the priority of identified threats or vulnerabilities. If one or a few hosts contain information that management views as critical, a host-based IDS may be warranted. If the information is less essential, other controls such as a firewall and/or filtering routers may be sufficient to protect the information. If an institution is primarily concerned with attacks from the outside or views the entire network system as critical, a network-based product may be appropriate. A combination of host- and network-based IDSs may also be appropriate for effective system security. Management should be aware that even after an IDS is in place, there may be other access points to the bank's systems that are not being monitored. Management should determine what types of security precautions are needed for the other access points.

The placement of the IDS within the institution's system architecture should be carefully considered. The primary benefit of placing an IDS inside a firewall is the detection of attacks that penetrate the firewall as well as insider abuses. The primary benefit of placing an IDS outside of a firewall is the ability to detect such activities as sweeping, which can be the first sign of attack; repeated failed log-in attempts; and attempted denial of service and spoofing attacks. Placing an IDS outside the firewall will also allow the monitoring of traffic that the firewall stops.

PART THREE – RESPONSE: Discusses implementing an incident response strategy for the response component of an institution's information security program.

INCIDENT RESPONSE

After implementing a defense strategy and monitoring for new attacks, hacker activities, and unauthorized insider access, management should develop a response strategy. The sophistication of an incident response plan will vary depending on the risks inherent in each system deployed and the resources available to an institution. In developing a response strategy or plan, management should consider the following:

- The plan should provide a platform from which an institution can prepare for, address, and respond to intrusions or unauthorized activity. The beginning point is to assess the systems at risk, as identified in the overall risk assessment, and consider the potential types of security incidents.
- The plan should identify what constitutes a break-in or system misuse, and incidents should be prioritized by the seriousness of the attack or system misuse.
- Individuals should be appointed and empowered with the latitude and authority to respond to an incident. The plan should include what the appropriate responses may be for potential intrusions or system misuses.
- A recovery plan should be established, and in some cases, an incident response team should be identified.
- The plan should include procedures to officially report the incidents to senior management, the board of directors, legal counsel, and law enforcement agents as appropriate.

Today's products not only can detect intrusions in real-time, but can automatically respond to intrusions. Depending on the software, information systems personnel can be notified on a real-time basis during an attack, rather than detect the attack afterward during a manual log review. Methods of notification can include e-mail, pager, fax, audio alarm, or message displays on a computer monitor. Responses can include shutting down the system, logging additional information, and disabling a user's account (e.g., by disallowing a particular user account or Internet address). Access can be disabled for a period sufficient for information systems personnel to review the attack information or verify the user. Also, an institution can add warning banners to protected systems, notifying users that they are accessing a protected computer system.

When determining an appropriate response, a distinction should be made between incidents in which actual changes to a system are suspected (e.g., changing audit logs) versus incidents in which system misuse is suspected (e.g., unauthorized system access). Attempts to actually change the system or data may warrant notifying a security officer, who could reconfigure the identified weaknesses and/or communication paths. An appropriate response to system misuse may include automatic log-off, warning messages, or notifying the appropriate personnel.

Not only are attacks often undetected, in many cases identified attacks are not reported. Institutions should develop a plan to respond to unauthorized activities and involve law enforcement when appropriate. Institutions should report suspected computer crimes and computer intrusions on Suspicious Activity Reports (SARs) in accordance with the guidelines outlined in Financial Institution Letter 124-97, “Suspicious Activity Reporting,” dated December 5, 1997.