BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM

WASHINGTON, D. C. 20551

DIVISION OF BANKING
SUPERVISION AND REGULATION

SR 97-32 (SUP)
December 4, 1997

TO THE OFFICER IN CHARGE OF SUPERVISION AND APPROPRIATE SUPERVISION AND EXAMINATION PERSONNEL AT EACH FEDERAL RESERVE BANK AND TO DOMESTIC AND FOREIGN BANKING ORGANIZATIONS SUPERVISED BY THE FEDERAL RESERVE

SUBJECT: Sound Practices Guidance for Information Security for Networks

Growth in the use of computer networks has heightened the interest of supervisors and managers of banking organizations in the quality and integrity of information security systems. The Federal Reserve System recognizes that effective and reliable information security policies and procedures are essential to maintaining public trust and confidence in our banking and financial system. Thus, it has a vital interest in encouraging banking organizations to take appropriate precautions as they increasingly provide services and information in electronic form and especially in the open environment of the Internet. Adverse financial, operational, reputational, and legal consequences can result from ineffectively managing the security of these networks and computers. Active board and management oversight are needed to ensure that risks are adequately assessed, that spending on information security is appropriate to reduce the risks, and that a comprehensive information security program is in place to provide protection.

In 1996, the Federal Reserve Bank of New York formed a team to benchmark sound information security policies and practices. The team interviewed a cross-section of Second District financial services institutions as well as security firms, service providers, common carriers, CPA firms, and other industry-related organizations. In addition, thirteen selected institutions were interviewed by teams from the Federal Reserve Banks of Chicago and San Francisco to validate the team's initial findings. The results are contained in the attached paper entitled "Sound Practices Guidance for Information Security for Networks." This SR letter and the sound practices paper should be distributed to appropriate examination personnel, and to the chief executive officer of each domestic and foreign banking organization supervised by the Federal Reserve.

The guidance presented in the paper does not constitute a regulation and should not be interpreted as such. Rather, the paper outlines the types of prudent and effective measures that financial services institutions have implemented, are in the process of implementing, or plan to implement to protect information and ensure its integrity, availability, and confidentiality. The key points

made in the paper are:

- *A strong information security program is essential*. A strong comprehensive information security program establishes the necessary structure and accountability to manage risks, and fosters awareness throughout the organization that information security is an important cultural value. A strong information security program includes active board and management oversight, policies and procedures, measurement and monitoring systems and ongoing internal controls. Boards of directors and senior management are responsible for ensuring that spending on information security is appropriate to the magnitude and nature of the risks.

- *Internal network security issues need special attention.* The vulnerabilities of internal networks may be less obvious to banking organizations than networks connected to the Internet, yet these internal systems are vulnerable to a wide variety of intrusion tactics. Internal attacks are potentially the most damaging because an institution's personnel, which can include consultants as well as employees, may have authorized access to critical computing resources.

- *Confidential information needs to be encrypted.* The confidentiality of data transmitted over public networks is vulnerable to risks in addition to those identified for internal networks. "Dedicated" or "leased" lines may provide an inappropriate sense of security. These lines use the infrastructure of public networks and therefore are vulnerable to the same attacks as the public networks themselves.

- *Internet connections need to be carefully constructed.* An institution's Internet site is exposed to worldwide attack. As more products and services are offered via the Internet, the opportunities for attack increase. The greatest risk is associated with sites that have a path to the institution's internal network, thereby providing unauthorized individuals with a link, however convoluted, to attack internal networks and gain access to an institution's information assets.

- *The backgrounds of employees in especially sensitive positions need to be checked.* Information technology personnel such as systems administrators, telecommunications support staff, systems programmers and others may have access to sensitive information, detailed knowledge about security methods and procedures, or both. Therefore, it is important to subject them to rigorous background checks.

- *Management must decide on benefits and costs*. Protecting networks to minimize financial, operational, reputational, and legal risks can require the dedication of significant resources. Senior

management is responsible for evaluating the costs and benefits of alternative security measures and deciding the best allocation of the institution's resources.

Although there are risks associated with private local and wide area networks and the Internet, they can be managed by a comprehensive information security program. Institutions should view sound practices in the context of their own needs and budgets and implement those that are appropriate.

Questions on the Federal Reserve Board's supervisory approach to information security matters may be addressed to Mr. Michael G. Martinson, Deputy Associate Director, Federal Reserve Board (202-452-3640). Questions on the contents of the paper may be addressed to Mr. George R. Juncker, Vice President (212-720- 6491), or its principal authors, Mr. Robert W. Dabbs, Assistant Vice President (212-720- 5937), and Mr. Joseph L. Galati, II, Examining Officer (212-720-7946), at the Federal Reserve Bank of New York.

Richard Spillenkothen
Director

ATTACHMENT TRANSMITTED ELECTRONICALLY BELOW

Suggested Transmittal Letter
to the Chief Executive Officer or General Manager of
Each Bank Holding Company, State Member Bank,
U.S. Branch and Agency of a Foreign Bank, and Edge Corporation

Subject: Sound Practices for Information Security for Networks

Dear _____:

The enclosed letter from the Federal Reserve Board's Division of Banking Supervision and Regulation and the accompanying paper, prepared by supervision staff of the Federal Reserve Bank of New York, contain important information on sound information security practices to address risks associated with computer networks. A version of this paper was distributed at a security conference sponsored by the Federal Reserve Bank of New York on September 24, 1997. Presentation materials from the conference are available at the Bank's web site at http://www.newyorkfed.org/pihome/news/speeches/.

The guidance presented in the paper does not constitute a regulation and should not be interpreted as such. However, the paper outlines the types of

prudent and effective measures that financial services institutions have implemented, are in the process of implementing, or plan to implement to protect information and ensure its integrity, availability, and confidentiality. In this connection, the paper may provide insights and assistance in designing an effective information security program and secure automation systems.

It is suggested that the letter and the paper be distributed within your organization to senior management and others with responsibility for network security.

Should you or your staff have any questions regarding this topic, please contact _____ at this Reserve Bank, or the contacts identified in the Board's letter.

Enclosures

Sound Practices Guidance for Information Security for Networks

Sound Practices Guidance for Information Security for Networks

Management Overview

Heightened supervisory interest in information security related to computer networks stems from the desire of the Federal Reserve System and the financial services industry to maintain trust in the banking system. The Federal Reserve System is interested in ensuring that banking organizations take all necessary actions to maintain the integrity of their computer systems and networks as they increasingly provide services and information in electronic form and especially in the open environment of the Internet. Adverse financial, operational, reputational, and legal consequences can result from ineffectively managing the security of these networks and computers. Active board and management oversight are needed to ensure that the risks are adequately assessed, that spending on information security is appropriate to mitigate the risks, and that a comprehensive information security program is in place to provide protection. In 1996, the Federal Reserve Bank of New York formed a team to benchmark sound information security policies and practices. The team interviewed a cross-section of Second District financial services institutions as well as security firms, service providers, common carriers, CPA firms, other industry-related organizations. The team consulted with 34 organizations, primarily in the Second District. In addition, thirteen selected institutions were interviewed by teams from the Federal Reserve Banks of Chicago and San Francisco to validate the team's initial findings.

The most widespread observation by the participants in the review was the importance of a comprehensive, management-directed information security program. A strong program fosters awareness throughout the organization that information security is an important cultural value, and establishes the necessary structure and accountability to manage risks. A strong information security program includes active board and management oversight, policies and procedures, measurement and monitoring systems and ongoing internal controls. The institutions that participated in the review recognized that irreparable financial, operational, reputational, and legal consequences can result from ineffective management of information security. Of particular importance, active board and management oversight ensures that the resources dedicated to information security are commensurate with the criticality of the information and the business processes at risk.

A second observation was that networks have the most significant inherent vulnerabilities and, therefore, require continuous attention and proactive measures. These measures include a combination of comprehensive information security policies, sound information security practices, compensating controls and

review mechanisms. Although the greatest potential risks are related to external open networks like the Internet, the team found that financial institutions are approaching the use of the Internet cautiously and are implementing information security measures that are commensurate with the services offered. The team believes that banking organizations may not recognize to the same degree the vulnerabilities of internal networks. Accordingly, the areas focused on in this report and recommended for close review by financial institutions are

- *Security of Internal Networks* - Attackers may gain access to networks and/or to systems on these networks, including value transfer systems[1] and systems with highly sensitive information and business processes, exposing institutions to credit, liquidity, reputational, operational, and legal risks.[2] These systems are most often publicized as being attacked, generally from internal sources, and are vulnerable to a wide variety of intrusion tactics.

- *Confidentiality of Information Transmitted Over the Public Networks*[3] *Without Encryption* - Institutions transmitting unencrypted data over public networks may be exposed to reputational and legal risks if the confidentiality of highly sensitive data is compromised.

- *Appropriate Architectures for Internet Connectivity* - Risks associated with Internet sites vary according to the levels of service offered. Sites with a path to the institution's internal network to provide a desired level of service also provide unauthorized individuals with potential access to the internal network and need the highest levels of protection.

This paper discusses these vulnerabilities in more detail and describes prudent risk management practices. Appendix A provides more detailed sound

---

[1] "Value transfer systems" encompasses money and securities transfer systems, and other applications that use these systems to effect a transfer of ownership of money or other assets from one party to another (e.g., loan, foreign exchange, and custody systems).

[2] These risks are defined and discussed in SR 95-51, "Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies."

[3] "Public networks" includes the communications infrastructure provided by regional operating companies and long distance carriers.

practices for protecting private local and wide area networks[4] and systems. Appendix B provides an overview of Internet technology and sound practices for protecting Internet sites and networks connected to the Internet. The guidance presented in this paper is not regulation and should not be interpreted as such. The sound practices reflect the types of prudent and effective measures that financial services institutions have implemented, are in the process of implementing, or plan to implement to effectively protect information and ensure its integrity, availability, and confidentiality.

Managing the Risks

Every institution must evaluate the risks it faces and its readiness to deal with them. To manage information security risks, it is first necessary to differentiate among their degrees of severity. With regard to the issues raised in this paper:

- *Not all networks are equally vulnerable*. The measures needed to secure networks vary according to the design and openness of the networks involved. The spectrum extends from tightly controlled, time-tested mainframe-centric networks to widely distributed networks with unsecured servers located in geographically dispersed locations. Most vulnerable is the Internet and, potentially, networks connected to it.

- *Not all systems are equally critical*. Systems capable of transferring ownership of money or other assets or that process official bank records carry a much higher degree of risk than systems providing local administrative automation services. Accordingly, measures to secure systems will vary in cost and complexity.

- *Not all data are equally sensitive*. The extent and expense of measures taken to protect data should be commensurate with their sensitivity. The spectrum of data sensitivity extends from highly sensitive data, which if made public could create serious credit, liquidity, reputational or legal risks, to data entirely appropriate for public dissemination. The spectrum of measures to protect information may extend from encrypting the data in storage and in transit across highly secured

[4]"Private local and wide area networks" refers to internal networks comprised of local area networks (LANs), and of LANs in geographically dispersed locations connected by public networks to form wide area networks (WANs). "Local area networks" are networks comprised of information systems resources including: servers (computers supplying processing resources to other network elements), printing and storage devices, and desktop systems.

network segments to making the information freely available on public Internet sites.

- *Management must decide on benefits and costs*. Protecting networks to minimize financial, operational, reputational, and legal risks can require the dedication of significant resources. Senior management is responsible for evaluating the costs and benefits of alternatives security measures and deciding the best allocation of their institution's resources.

Information Security Risk Management Practices

The foundation of effective information security management is a comprehensive policy sponsored by the board of directors and executive management. Information security risk is further mitigated by a management structure that effectively executes information security policies and adequately identifies, measures, monitors, and controls the information security risks involved in its various businesses.

The level of technical knowledge required by directors and senior managers varies depending on the particular environment. Directors and senior managers of institutions that conduct a broad range of technically complex activities, for example, cannot be expected to understand the full details of the institution's information security procedures or the precise ways information security risks are mitigated. They should, however, have a clear understanding of the types of information security risks to which the institution is exposed and take an active oversight role by receiving periodic briefings that identify the material risks in terms that are meaningful to them. In fulfilling this responsibility, directors and senior managers need to develop an appropriate understanding of the risks their institutions face, possibly through information provided by auditors and outside experts. Based on this knowledge, directors and senior managers should provide clear guidance regarding acceptable levels of security over the institution's information assets and ensure that they implement the procedures and controls necessary to comply with established policies. Principles of sound risk management apply to the entire spectrum of security risks facing a financial services institution including the security of data processing resources, information assets, and delivery channels.

A sound information security risk management system has the following elements:

- Active board and senior management oversight;

- Policies, procedures, practices and penalties;

- Risk measurement, monitoring, and management information systems; and

- Internal controls and audits.

Active Board and Senior Management Oversight

Boards of directors have ultimate responsibility for the level of information security risk taken by their institutions. Accordingly, they should approve the overall business and technology strategies and broad information security policies of their organizations.

Active oversight is demonstrated by boards of directors that:

- Understand the types of information security risks inherent in the business activities and endeavor to remain informed about these risks as products and services are launched and improved, and new technologies and delivery channels are introduced.

- Review and approve information security policies to address information security risks inherent in the institution's credit, investment, funding, trading, fiduciary and other significant applications and processing activities.

- Reinforce the strategic stature of information security throughout the organization by commitment to and participation in setting corporate security direction.

- Review and approve levels of risk exposure deemed acceptable as changes are planned in the institution's products and services, technologies, and outsourcing arrangements.

- Review and approve the institution's internal audit program for appropriate scope and frequency concerning compliance with information security policies.

Senior management should take ownership of their institution's security risks and exercise managerial oversight over information security activities, even though such activities may be delegated to others. In addition, senior management should:

- Provide direction for consistent levels of information security throughout the organization by establishing a corporate information security function and appointing an information security officer.

- Handle information security as a strategic business concern, not just a technical issue.
- Delineate authority and responsibility, while retaining accountability for managing information security risk.

- Staff security functions with competent personnel who have the appropriate knowledge, experience, and expertise needed to address the risks faced by the institution's technical and business activities.

- Link information security to performance. The institution's code of conduct and the personnel appraisal process should address security expectations. Similarly, judgements of the performance of business units should consider results of information security audits and compliance reviews.

- Assure timely response to changes in information security risks due to changes in technology or from innovations in its markets. Ensure that the infrastructure and internal controls are in place.

- Ensure that crisis plans, including management escalation, are formulated and tested for information security incidents.

Policies, Procedures, Practices, and Penalties

Once the security risks that arise from the institution's business activities and specific technical environments are properly identified, policies and procedures provide detailed guidance for the consistent application of corporate and business line information security strategies.

The effectiveness of information security risk management depends on the communication of policy, procedures, practices, and penalties as well as the support of the board of directors and executive management. Several processes necessary to formulate and maintain information security policies include:

- ***Risk Assessment*** - inventory systems, applications and data sources. Assess criticality and sensitivity. Evaluate information for the level of protection required (data classification or data typing).

- ***Framework*** - develop and coordinate the four "P's": Policies, Practices, Procedures and Penalties. Define information security measures, violations, and penalties.

- ***Delegation*** - assign individual authority, responsibility and accountability for information security and explicitly communicate to all appropriate individuals.
- ***Implementation*** - given an information security framework approved by the board of directors and supported by executive management, implement the information security policy on a timely basis.

- ***Awareness*** and ***Training*** - train for positive re-enforcement of the program. Continual awareness is essential for maintaining prescribed information security levels.

The minimum elements of an information security policy include:

- Delineating clear accountability and lines of authority across the institution's businesses and information security activities.

- Integrating information security policy within overall business and technical strategies and risk management practice, and applying policies and procedures consistently across business activities.

- Setting review processes for activities and technologies new to the institution to ensure that infrastructures necessary to identify, monitor, and control information security risks are addressed in advance of their introduction.

- Revising policies based on internal experience and relevant industry advisories addressing breaches, safeguards and countermeasures.

- Establishing a legal basis for enforceability and prosecution, to protect an organization's informational property.

Risk Measurement, Monitoring and Management Information Systems

Effective risk monitoring requires institutions to identify and measure significant information security risk exposures. Consequently, risk monitoring activities must be supported by information systems that provide directors and senior managers with timely and reliable reports on the performance of information security measures. Daily activities should be closely monitored and reports of

violations and exceptions should support the needs of management and information security.

Appendix A details several objectives for measuring, monitoring and reporting information security performance through risk monitoring practices, including logging, activity, violation, and exception reports and the use of audit reduction tools to extract pertinent information and identify new information security issues. Other objectives include:

- Monitoring exposures to ensure ongoing compliance with policies, practices, and procedures with the enforcement of penalties for information security breaches.

- Rendering reports that are complete, accurate, timely and present sufficient information for decision-makers to identify adverse trends and to evaluate adequacy and effectiveness of preventive, detective and corrective measures.

- Moving toward the use of real-time intrusion detection to identify and monitor not only violations but patterns of anomalous activity, especially for critical systems.

- Reviewing and changing security profiles to reflect employee resignations, transfers, and changes in job responsibilities.

- Testing the strength of information security through compliance audits and penetration tests by trusted parties.

Internal Controls and Audits

An institution's internal control structure is critical to the safe and sound functioning of the organization generally and to its information security risk management system in particular. A secure operating environment requires an effective system of controls to prevent, detect, and correct information security breaches. The appropriate delegation of authority, as reflected in security profiles, is equally important.

Segregation of duties is another fundamental element of a sound risk management and internal control system. Failure to implement and maintain adequate segregation of duties with respect to business activities and information security administration, including maintenance of individual security profiles, constitutes an unsafe and unsound practice and can lead to serious losses or

otherwise compromise the financial integrity of the institution.

When properly structured, a system of information security measures effectively protects an institution's information assets and processing environments. An independent internal or external auditor should test the information security schemes. The results of audits or reviews should be adequately documented along with management's response. Moreover, negative or sensitive information security findings to be reported directly to the board of directors or to the relevant board committee.

Summarizing the specific objectives described in Appendix A, a robust internal control environment:

- Addresses the integrity, accessibility and confidentiality of official institution records as they are originated, processed, transmitted, stored, archived, and destroyed.

- Establishes clear organizational lines of authority and responsibility for monitoring adherence to policies, procedures, and practices, as well as the handling of violations.

- Provides sufficient independence of information security administration from business activities, and adequate segregation of duties throughout the organization to preserve a system of checks and balances.

- Assures internal and regulatory reporting of information security incidents that are reliable, accurate, and timely.

- Affords independence and objectivity of internal audit and control review practices and provides internal audit coverage of adequate scope, frequency, and procedural depth.

- Takes information security into consideration in crisis management, contingency planning, application development, facilities management, new business development, and new delivery channels.

Areas Recommended for Review by Financial Institutions

Security of Internal Networks

The security of private local and wide area networks is an area that needs to be reviewed and evaluated carefully because, as security experts' surveys

report, the majority of attacks come from internal sources. Internal attacks are potentially the most damaging because an institution's personnel, which can include consultants as well as employees, may have authorized access to critical computing resources. Combined with detailed knowledge about an institution's practices and procedures, an internal attacker could access value transfer systems directly, or exploit trusted relationships among networked systems, to gain a level of access that allows the attacker to circumvent established security controls. After circumventing the security controls on a value transfer system, the attacker could transfer money or other assets, or cause money or other assets to be transferred, to another party.

Internal local and wide area networks are vulnerable to attack in a variety of ways, including those listed below which were identified by the organizations participating in the study:

- Intercepting authentication or other sensitive information, often using software or hardware devices known as "sniffers." "Sniffers," originally designed to diagnose network-related problems, are specialized software or hardware tools that intercept information in transit over networks.

- Guessing passwords that protect accounts or system services, particularly default passwords that have not been changed.

- Retrieving and decoding password files ("brute force attacks").

- Sequentially or randomly dialing every number on a telephone exchange (known as "war dialing") to detect unprotected modems at desktop systems, servers or routers to gain access to, or control over, networks.

- Deceiving the network so that it recognizes an unauthorized, possibly external, desktop system as an authorized, internal desktop system ("spoofing") to gain unauthorized access to networks and/or sensitive data.

- Attempting to gain information or access by posing as a help desk or repair person, or as an individual in a position of authority ("social engineering") to gain access to networks, desktop systems and servers.

- Inserting software, which does not disrupt normal transactions, into desktop systems or servers to gather information or perform

surreptitious acts ("Trojan horses") to gain control of the desktop system or server.

- Intercepting authenticated sessions to preempt access by a desktop system to gain control of a session with access to highly sensitive information or business procedures ("hijacking").

- Exploiting vulnerabilities in operating systems to gain control of computers.

Among the sound practices, the most important defenses against these attacks is the encryption of highly sensitive data in storage and in transit across networks and the use of strong authentication (e.g., one-time passwords) to control access to critical systems and business processes. Strong authentication and encryption provide additional layers of security to institutions' most valuable assets. In addition, the wide range of other security practices outlined in Appendix A also are important. They have the added advantage that an attacker who penetrates an internal network is still faced with formidable obstacles in getting to an institution's sensitive data, critical business processes, or value transfer systems.

Confidentiality of Information Transmitted over Public Networks Without Encryption

The confidentiality of data transmitted over public networks poses additional risks to those identified for internal networks. "Dedicated" or "leased" lines may provide an inappropriate sense of security. These lines use the infrastructure of public networks and therefore are vulnerable to the same attacks as the public networks themselves. Although the security of public networks is upgraded constantly, they have many of the same characteristics as local and wide area networks and regularly are subjected to the same types of attacks that are described above. In addition, lines may be tapped, and at some point in traversing the network, data may be transmitted via microwave, wireless or satellite links that are susceptible to being intercepted. Finally, key public network operations and support personnel may be able to access highly sensitive data being transmitted over the networks.

Confidential data transmitted via public networks may be intercepted or compromised by individuals for whom the data are not intended. Therefore, it is prudent to encrypt sensitive and highly sensitive data transmitted via public networks.

Appropriate Architectures for Internet Connectivity

An institution's Internet site is exposed to worldwide attack. As more products and services are offered via the Internet, the opportunities for attack increase. The greatest risk is associated with sites that have a path to the institution's internal network, thereby providing unauthorized individuals with a link, however convoluted, to attack the internal network and gain access to an institution's information assets.

There are three types of Internet sites:

- *Information-Only Sites* provide information about the institution and its products and services, but provide no interactive capability. Normally, these sites do not provide paths to internal networks and therefore the potential for loss of money and other assets is low. The potential for significant reputational risk exists, since a successful attacker may alter information on the site.

- *Information-Exchange Sites*, in addition to providing information, allow customers to send information to the institution or to make inquiries about their accounts. These communications may take the form of:

  - E-mail;
  - on-line forms (e.g., loan applications); and
  - account queries.

  These sites may provide a path to internal networks via e-mail and attachments and therefore represent a higher level of risk than information-only sites. There is potential for infection of the network by viruses; thus implementation of virus protection measures is important. If the form and account-information updates are not via a direct connection to the internal network, they do not pose additional risk. However, if there is a direct connection, the measures to protect the site should be the same as for a fully transactional site.

- *Fully Transactional Sites* provide the capabilities described above as well as on-line, real-time account queries, transfer of funds among accounts, bill payments, and other banking services. These capabilities typically are provided by interactive connectivity between the Internet site and the bank's internal network and therefore represent the highest potential risk of successful attack on an internal network and the potential for the loss of money, other assets, and highly sensitive information. These sites require the most rigorous level of protection.

The level of protection of an Internet site should be commensurate with the degree of risk presented by the level of services offered and the value of assets at risk. Detailed recommendations for the appropriate measures to protect sites offering each of these levels of service are provided in Appendix B.

Summary and Conclusions

Although there are risks associated with private local and wide area networks and the Internet, they can be managed by a comprehensive information security program and the judicious use of internal controls complementing the careful implementation of the appropriate sound practices in Appendices A and B. Institutions should view these sound practices in the context of their own needs and budgets and implement those that are appropriate. In addition, implementing compensating controls may, in some cases, address information security issues.

Appendix A

Sound Practices for Private Local and Wide Area Networks: A Senior Management Perspective

This Appendix presents sound practices for enhancing the security of private local and wide area networks. Because this appendix is intended for senior management, the practices are presented largely at a conceptual level with explanatory material for each recommendation.

These sound practices are not regulation and should not be interpreted as such. They reflect the types of prudent and effective measures that security-conscious financial services institutions have implemented, are in the process of implementing, or plan to implement to effectively protect information and ensure its availability, confidentiality, and reliability. Institutions are not expected to implement all of these sound practices; they should view them in the context of their own needs. In addition, one or more of the sound practices may address the same security vulnerability using different techniques, and some vulnerabilities may be addressed by implementing compensating controls. Four sound practices are viewed as essential, however: the development of a comprehensive information security policy, data classification, encryption of highly sensitive data, and strong authentication for controlling access to critical systems and business processes.

Appendix A is organized by the following categories:

- Confidentiality
- Access Control, with a section on password policies
- Configuration Control
- Security Policies
- Network Security and Monitoring
- Personnel
- Business Continuity

Confidentiality

Classify data, or perform "Data Typing," to define the sensitivity of data.

Not all data are equally sensitive. To identify the data that need to be protected, categorize data according to a security classification. The number of classification levels will vary from institution to institution based on the business needs of each. For the purposes of this paper, data are classified according to three levels: "highly sensitive," "sensitive," and "public." "Highly sensitive" data, if made public, would cause the institution major embarrassment and/or financial loss (reputational, credit and liquidity risks). "Sensitive" data, if made public, would result in manageable embarrassment and/or financial loss.

Data classification is an essential sound practice; it is the foundation for successfully enhancing the security of private local and wide area networks: an institution can not properly protect its most sensitive and valuable information resources without first identifying them.

Encrypt highly sensitive data when stored and transmitted across private local and wide area networks.

Private local and wide area networks are vulnerable to attacks. To minimize the risk from attacks by unauthorized individuals, an essential sound practice is to encrypt highly sensitive data in storage and transmission across private local and wide area networks. In addition to protecting the data from access by internal attackers, encryption also provides protection if an external attacker gains access to an institution's internal network. An attacker's access to institutions' highly sensitive data will be severely inhibited by strong encryption.

The element that is used to uniquely encode (encrypt) data and subsequently decode (decrypt) the encrypted data is known as the "cryptographic key." The "cryptographic key" must remain secret to protect the integrity of the encrypted data. Therefore, effective key management is an essential element of strong encryption. Among the elements of effective key management are: 1) protection of the keys, in storage and distribution, against unauthorized access or modification, and 2) periodically changing the cryptographic key. The sensitivity of the data determines the frequency of the key changes. For highly sensitive data, the cryptographic key should be changed every time the data are accessed.

Encrypt all transmissions of highly sensitive and sensitive data over public networks.

Although the security of the public network is upgraded constantly, the network also is vulnerable to attack using many of the same techniques used in attacking private local and wide area networks. Therefore, it is prudent to assume that highly sensitive and sensitive data transmitted via the public network may be intercepted by individuals for whom the data are not intended.

It also should be recognized that the data transmitted over dedicated or leased lines are likely at some point to be transmitted via the infrastructure of the public network and therefore vulnerable to the same attacks as is the public network itself.

To protect data that may be intercepted by unauthorized individuals, encrypt the data as they transverse the public network.

Use network switches, and/or intelligent hubs with the ability to restrict desktop systems from intercepting messages intended for other devices.

"Hubs" provide network connectivity for desktop systems; that is, desktop systems are connected to hubs, which in turn are connected to the network. A disadvantage of this arrangement is that every desktop system connected to a hub has access to ***all*** of the traffic on that segment of the network. Thus, a desktop system connected to a hub with the appropriate hardware or software can "sniff" (intercept and decode) all of the traffic on that network segment. Some intelligent hubs allow a desktop system to receive only the data intended for it (i.e., data with the desktop system's network address). Also, network connectivity for desktop systems can be provided by "network switches." Network switches direct messages with the proper network address to individual desktop systems. Therefore, some intelligent hubs and network switches only transmit to a desktop system messages intended for it. This eliminates the vulnerability that users may sniff traffic that is not addressed to their desktop system.

Access Control

Use strong authentication to: restrict access to critical systems/business processes and highly sensitive data; control remote access to networks; and grant access to the control functions of critical network devices.

Because of the vulnerability of reusable passwords, control access to

critical systems, applications, data, and network functions by strong authentication. "Strong authentication" includes, but is not necessarily limited to, "one-time" passwords, digital certificates, and biometrics.

Passwords that are used only once and change for each user access session are known as "one-time" passwords. These passwords are generated by programmable devices, usually chip-cards (also known as "smart cards" or "tokens"). In some implementations, access to the programmable device is controlled by a password for additional protection.

There is emerging technology for other forms of strong authentication, including digital certificates, which are discussed further in Appendix B, and biometrics. "Biometrics" is an identification process based on physical characteristics unique to the user, such as finger prints, patterns associated with the voice, retina or iris, and facial characteristics. These technical developments should be followed as they may offer valuable additional security features that warrant implementation.

Segment networks to prevent interception of data.

Since internal networks are susceptible to sniffers and other techniques for intercepting highly sensitive and sensitive data, separate internal networks into segments so that dissemination of these data is restricted to a controlled subset of users. This can be accomplished by physically separating networks with bridges, routers, firewalls[5] or other access control devices to prevent users from intercepting data on segments for which they are not authorized.

Meticulously change ALL default passwords on critical network components.

Firewalls, servers, and other critical network components when delivered typically have a number of default passwords provided in the documentation or that can be guessed easily by attackers. Change ALL of these passwords.

Centralize all critical devices supporting private local and wide area networks in "glass houses" to enhance physical access control.

---

[5]As institutions move toward Internet technology for their internal networks (intranets), the more it introduces the security issues associated with the non-proprietary (open) technology of the Internet. Therefore, many of the security techniques used to protect Internet sites, such as firewalls, may also be used to enhance the security of internal networks. See Appendix B for a discussion of firewall technology.

Denying attackers physical access to critical systems and their consoles (i.e., the keyboard or desktop systems used to control the servers) significantly decreases the opportunities to penetrate and/or gain a level of access that circumvents the system's security controls. Maintaining good physical access control is most easily accomplished by centralizing all critical network devices, firewalls and servers in "glass houses"; that is, in areas that are physically and environmentally secure, often staffed 24 hours per day. Centralizing servers also allows more effective maintenance of server functionality, since distributed servers often are unattended after business hours. Using "glass houses" is not a recommendation to centralize distributed processing systems. For geographic or other business reasons, a financial services institution may choose to have a number of "glass houses."

Limit control of servers to local consoles in the "glass house."

To limit console-based attacks on servers, particularly attempts to retrieve restricted data such as password files, limit access of server-control devices to consoles physically attached to servers located in the "glass houses." This allows strict control of physical access to the console. In addition, password protect the console screen. Change each password often. If it is necessary to remotely administer servers, use strong authentication and encrypted sessions to control access by the remote device.

Centralize the connection points of an institution's network in secure locations.

Physically secure and closely monitor network connection points, since they are vulnerable to "sniffing". Install the network connection points in physically secure closets or in "glass houses" along with the other critical network devices.

Create and maintain security profiles for all users.

Security profiles define users' access to facilities and data based on their business responsibilities. They streamline the process of granting and revoking access rights to facilities and data, by grouping the rights together according to job function. When employees change jobs, changing their security profile promptly is essential to prevent continued access to facilities and data that are no longer appropriate. When employees leave, promptly deleting all of their access rights is essential.

Follow the development of centralized user security profile management systems that will allow employees' access to critical systems to be changed or deleted if the employee changes responsibilities or resigns.

Because of the complex environment of networks, many security profiles are required. Typically, employee's have a security profile on each system in the network to which they have access. To exercise better control over these profiles, commercial software is being developed that centralizes security profile management. If an employee changes responsibilities or resigns, this software will provide the capability to grant, change, or deny access to all systems by updating the user's centralized security profile. Although the technology is not yet mature, if developments result in a robust centralized management capability, the resulting benefits for enhanced security may warrant implementation.

Protect against loss or corruption of critical business logic and highly sensitive data residing on desktop systems.

Because of the susceptibility of desktop systems to theft, access by unauthorized personnel, and destruction or failure, minimize storage of highly sensitive data or critical business processes on desktop systems. Promote implementing critical business processes and associated data on servers located in "glass houses." If business reasons require highly sensitive data or critical business processes to reside on desktop systems, protect them by access controls, encryption, and periodic backup procedures.

Control access to desktop systems connected to critical networks or network segments and desktop systems supporting highly sensitive data or critical business processes by a power-on logon ID/password combination or locked office.

Most desktop systems have a feature that requires a password to gain access when the device is powered up. Implement this feature to prevent unauthorized personnel from gaining control of desktop systems connected to critical networks or network segments, and to desktop systems supporting highly sensitive data or critical business processes. Bypassing this feature requires taking the battery out of the desktop system and waiting about twenty minutes, therefore increasing the probability that the unauthorized person would be caught during the intrusion attempt.

Provide a central dial-in and dial-out modem pool for remote access. Strictly control outside access from networked desktop systems that connect to the public switched network via analog lines or digital PBXs[6].

Network-connected desktop systems with modems that make calls to and from the public switched network represent one of the greatest vulnerabilities to internal networks. Many institutions' security safeguards can be circumvented by an attacker gaining access to, and control of, a network-connected desktop system via an external modem. Virtually all laptop computers have modems in them and there is a growing trend to use laptops also as desktop systems through "docking stations." Therefore, remote access to an institution's internal network must be controlled rigorously. Provide remote access to networks by modem pools that are isolated from the internal network via firewalls and/or other appropriate security measures. Modems (using analog telephone lines or A/D converters connected to digital PBXs) attached to networked desktop systems should be the exception and rigorously controlled.

It should be noted that a typical standard for modem-pool controllers to time out dial-in connections that are unexpectedly disconnected is 16 minutes. During this period, if attackers gain access to the modem to which the disconnected line was attached, they have the same access privileges as the user who lost the connection. Consider shortening this time-out period.

Periodically "war-dial" all the numbers on an institution's telephone exchange to detect unauthorized modems.

"War-dialing" consists of dialing each number on an institution's telephone exchange either sequentially or randomly to detect the existence of modems. Perform war-dialing periodically to detect and eliminate unauthorized modems.

Implement time-of-day controls for access to desktop systems connected to critical networks or network segments, where feasible, to eliminate unauthorized after-hours network access.

---

[6]Many large financial institutions have internal telephone switching systems (private branch exchanges or PBX's) that use digital computer technology. These telephone lines cannot be used with modems without an analog/digital (A/D) converter. An analog line is often run to the location of the desktop system instead of providing an A/D converter. Older PBX's often use analog technology. Then, a desktop system with a modem can be connected directly to the line attached to the telephone handset.

To prevent after hours access to critical networks by unauthorized personnel, allow access to desktop systems connected to these networks or network segments during business hours only. It will be necessary to implement other access control mechanisms for remote access users. If it is necessary for individuals to use their desktop systems connected to critical networks or network segments after normal business hours, carefully control access on an exception basis.

Provide desktop systems with an automatic time out feature that makes them inaccessible to an unauthorized individual after a period of keyboard inactivity.

Because of the risk associated with inappropriate use of unattended, logged-on desktop systems, make them inaccessible after a period of keyboard inactivity. The length of this period should be determined by the sensitivity of the application; for extremely sensitive applications, (e.g., money transfer) the period of inactivity should be short.

Consider requiring periodic reauthentication of highly sensitive sessions to ensure a session has not been hijacked.

Hijacking occurs when an attacker disables a user's desktop system after an authenticated session with a highly sensitive database or system has been established, and then intercepts the responses from the application and responds in an appropriate manner to maintain the session. The user whose desktop system has been disabled may not take action to determine the cause of the lost session soon enough to prevent the hijacker from accessing the highly sensitive data or system. The hijacker's access can be limited by requiring periodic re-authentication for the continuation of the session.

Control powerful utilities that provide unrestricted access to highly sensitive and sensitive data.

Some utilities provide unrestricted access to system commands and data to "super users" (i.e., system administrators). Take great care when implementing utilities that give super users these capabilities: implement compensating controls such as separation of duties to limit their capability for autonomous actions or frequently review logs of super-user actions.

Provide the same level of physical and logical access control to backup files of highly sensitive and sensitive data as for the production versions.

Backup files of highly sensitive and sensitive data, particularly at off-

site locations, must receive the same level of protection as the production versions of the data.

Remove all highly sensitive and sensitive files from hard drives before disposing of obsolete desktop systems.

Obsolete desktop systems that are sold, contributed, or discarded may have highly sensitive or sensitive data on their hard drives. Ensure that proper measures are taken to remove all traces of these files so they can not be recovered. In some cases, physical destruction of the hard drives should be considered.

Password protect access to notebook computers and encrypt all highly sensitive and sensitive files on the computers' hard drives.

Because of the susceptibility of notebook computers to theft, take measures to minimize the opportunities for thieves to obtain highly sensitive and sensitive information contained on portable computers. The first line of defense is to require a logon ID/password combination to gain access to the PC's operating system. Beyond that, encrypt highly sensitive and sensitive business files so that if the notebook computer is stolen and successfully penetrated, the ability of the thieves to access highly sensitive and sensitive data is inhibited.

Password policies

Password policies are a subset of access controls. Although access to critical information systems infrastructure elements is best controlled by strong authentication, reusable passwords may be adequate for controlling access to less critical elements, so long as robust password policies are in place. In many instances, access may be controlled by a combination of strong authentication and reusable passwords.

Establish an effective password policy.

An effective password policy will require

- Passwords to have a minimum length, which may vary by institution, and consist of a combination of numbers, letters and symbols.

- Systems that automatically prompt users periodically to change their passwords with a frequency that will vary by institution and by the criticality of the information systems infrastructure elements being

protected.

- Users not sharing their password with any other individual and never writing the password down.

- Users not using passwords that are obvious or easily guessed.

Encrypt reusable passwords in transmission and storage.

Because of the susceptibility of networks to sniffing, hijacking, Trojan horses and other attacks, encrypt reusable passwords in storage and in transit through the network or use one-time passwords.

Select security subsystems and applications that provide a password history to prevent the reuse of recently used passwords.

To prevent users from reusing recently used passwords, select security subsystems and applications that maintain a password history. This history can be based upon time (e.g., for one year) or by retaining a specified number of previously used passwords.

Use commercially available applications to test the validity of users' passwords.

Applications are available that will test for users' passwords that are easily guessed or trivial. Use these applications to screen users' passwords as they are created to ensure, for example, that no passwords are used that match words in the dictionary and therefore are susceptible to "dictionary attacks."

Disable user accounts after a period of inactivity; purge them after a lengthy period of inactivity.

To ensure that a system does not contain old, unused user accounts, deactivate any that have not been used within a reasonable period of time. This period will vary by institution. If a user account continues to be disused, purge it from the system. However, it is important to check with the owners of the resources to which the user had access to ensure that the user is not the sole means of access to those resources.

Disable user IDs after multiple unsuccessful logon attempts, and notify the security administrator when this threshold is reached.

To prohibit attackers from using automated programs attempting to

guess a user's logon ID/password combination, implement a threshold, which will vary by institution, after which the logon ID is disabled. Advise the system administrator when the threshold is reached to allow the system administrator to investigate the situation. Review logs to detect multiple attempts at guessing users' passwords that avoid reaching the threshold in any one session. Care should be taken when applying this practice to system administrative accounts so system administrators will not be locked out if they forget their passwords.

Display the date and time of the user's last successful logon access and the number of unsuccessful logon attempts.

In order for a user to detect unauthorized users that have illicitly obtained a valid password, display the date and time of the last successful logon each time the user signs on. Train users to observe this date and time and to report any anomalies. Report the number of unsuccessful logon attempts since the last successful logon so that users will be able to determine that someone is attempting to guess their logon ID/password.

Follow the development of "Single Sign on" products.

There are products available and under development that allow users to sign on to a network once, providing access to all applications for which the user is authorized, rather than the user having to sign on multiple times when accessing different applications. Although this technology is not yet mature enough for wide-spread implementation, particularly for critical systems, it may warrant consideration when robust, secure versions are available. In addition to operational efficiencies, single sign on users are less likely to write down their passwords where they can be obtained by unauthorized users.

Configuration Control

Centralize the servers supporting internal networks in "glass houses" to enhance configuration control.

One of the most important attributes of a secure internal network is the proper configuration of the servers supporting the network. Many security breaches on networks are the result of improperly configured servers. If the servers supporting internal networks are distributed throughout an organization, the problem of maintaining properly configured servers is exacerbated because:

- The administrators of distributed servers may not have the level of training and expertise necessary to properly configure and maintain

them.

- Physical access to the servers is harder to control, which increases the potential for an unauthorized person to gain access to the server's console and, by guessing or otherwise obtaining the system administrator's password, gaining unauthorized access to the network and its servers.

By placing the servers in "glass houses," the institution can more easily:

- Ensure that the servers are configured to provide a consistent level of security throughout the organization.

- Update the system or network operating systems or application software on the servers in a timely manner. This is an important capability when a vulnerability in one of these areas is detected and a software update is required to eliminate it.

If it is not practicable to consolidate remote servers in a local "glass house," it is important to ensure that the remote servers' configurations provide a level of security consistent with the institution's standards. They also should be promptly updated when security problems are resolved in operating systems or applications software.

Periodically test the servers' configuration.

Network administration can be complex, presenting opportunities for configuration and administrative errors. In order to detect these errors, run security assessment tools that look for administrative and configuration weaknesses as well as security vulnerabilities, such as the existence of vendor-supplied default passwords. Tools are available to perform these functions for internal and external networks, network servers, and database management systems.

Due to the potential for inadvertent error or automatic reset of default options during modification of servers, run configuration tests against servers after ***any*** change to ensure that effective security remains intact.

Security Policies

Perform a detailed assessment of potential network information security risks

Because of the vulnerability of networks to attack, it is appropriate to perform detailed risk assessments of institutions' internal networks and use of the Internet to identify the areas where additional security measures or compensating controls are necessary.

Implement a comprehensive information security policy.

There are many issues that should be addressed in an institution's formal information security policy. At a minimum, policies should include the following:

- An introduction -- including a statement of board of directors and executive management support.
- Terms and definitions -- to provide clarity to the policy.
- Purpose -- to focus on the key areas of security concerns.
- Scope and Objectives -- to outline management's goals.
- General Policies -- including detailed and consistent security standards and how information will be protected.
- Specific Policies for Certain Services -- to identify unique situations (e.g., Internet usage).
- Roles and Responsibilities -- to identify all individuals involved and their duties including owners, custodians, administrators and users. Among these roles and responsibilities are:
    - Establishing a centralized corporate security function and/or appointing an information security officer to establish institution-wide security standards.
    - Assigning specific business areas responsibility for the ownership of the security of their data and for the prompt implementation of institution-wide security policies.
    - Ensuring that information security receives proper attention at the highest levels of the organization, preferably with the board of directors or audit committee. This will heighten security awareness at the most senior levels and reinforce the support these programs receive across all levels of the organization.

- Ensuring adequate training is provided to all employees to permit them to properly fulfill their information security responsibilities.

- Mechanisms to monitor adherence to established policies.

- Enforcement procedures that outline the penalties associated with security breaches.

- Crisis-management process -- to identify the steps to be taken if there is a security breach.

Virtually every institution visited sited a formal information security policy as an essential sound practice.

Consider requesting that vendors ship all products with default security measures as "everything denied."

Most vendor products are shipped with the security protections set to "everything allowed." Although it simplifies the installation, it makes it much more difficult to configure complex systems properly for optimum security. A better choice is for products to be shipped with "everything denied," which then requires the security administrator to enable those, and only those, services required for business purposes. Also, require certification by the vendor that the product is virus-free and contains no undocumented "back-doors."

Evaluate off-the-shelf or "shrink-wrapped" software with regard to its security features.

Give the same emphasis to the security characteristics of commercial off-the-shelf software as is given to its functional capabilities. Develop a checklist of the required security features of commercially available software. Test the security features to ensure that they are consistent with the vendor's representations.

Maintain current and accurate software inventories of applications, operating systems and utilities.

Institutions must have current and accurate software inventories so that if a weakness is detected in an operating system, application or utility, the location of the version of the software with the weakness can be identified and updated rapidly and correctly.

Perform due diligence with regard to service providers' security measures and require a comprehensive contract with service providers that covers security issues.

If an institution's activities are outsourced, carefully review the service provider's security arrangements. If the necessary expertise is not available in-house, retain an independent security consultant to perform this review. Require that the service provider meets the institution's security standards. Require a comprehensive contract that includes security issues.

Require contractual commitments from entities to whom banking services are provided to maintain a specified level of security.

Networks are only as secure as their weakest links. Therefore, when supplying services to other entities that involves linking networks, require the other entity to maintain an adequate level of security to protect the service-providing institution's network.

Implement a change-control mechanism that maintains control of changes to software and security mechanisms.

To minimize the opportunities for individuals in trusted positions to make surreptitious changes to operating systems, applications, or security procedures, implement an effective change control procedure to maintain control of any changes to the system, applications, or security procedures. After any changes, have users of the system rigorously test and verify all changes.

Create a crisis management procedure.

Create a crisis management procedure that includes:

- Mechanisms for recognizing a crisis.
- A "chain of authority" so prompt action can be taken, if necessary.
- The existence of an emergency response team with a clear designation of who is in charge and who is capable of making decisions.
- Coordination with the institution's disaster recovery plan.
- Evidence collection and preservation, not only for possible prosecution of attackers, but also to perform meaningful postmortem reviews of the crisis.

Network Security and Monitoring

Aggressively monitor system activity

There is a consensus that it is impossible to stop entirely well financed, highly skilled attackers. The objective is to have sufficient obstacles in place to slow attackers down enough so they can be detected and defensive measures can be taken. In order for this strategy to be effective, it is necessary to aggressively monitor system activity to detect anomalous events that may indicate that an attack is underway. Currently, monitoring largely consists of reviewing system logs (see below). Follow the development of real-time intrusion detection tools, which, as they become more effective, may provide powerful mechanisms for detecting attacks in progress.

Select system elements at critical control points (i.e., servers and firewalls) that provide logs of user, network and applications activity.

In order to detect anomalous activities that may indicate that an attack has been conducted or is underway, have detailed logs of user, network, and application activity. Due to the voluminous nature of these logs, use audit reduction tools to "reduce" these logs to manageable proportions. Audit reduction software scans logs for anomalies and patterns indicating suspicious or unusual activity, eliminating known acceptable patterns. Select software that notifies the systems administrator if highly unusual or dangerous patterns are detected. In addition to the use of audit reduction software, the periodic review of logs by a knowledgeable system administrator is invaluable. Since the nature of attacks changes over time, reviews by an experienced system administrator may detect patterns indicating an attack attempt that is not recognized by the audit reduction software.

Provide virus scanning software at critical entry points, such as remote-access servers, and/or provide each desktop system on the network with virus scanning software.

The detection of viruses in e-mail attachments is essential for institutions that allow e-mail from outside the organization to individuals or service areas within the organization. Internet access, if provided to employees, is another potential source of viruses. Virus detection can be done at the entry point (i.e., at the remote-access server), at the desktop, or both. It is highly desirable to have virus detection software on each desktop system and on each notebook computer. However, if virus detection is provided only at the entry point, additional awareness training must be given to employees with regard to checking diskettes for viruses (see below). Update virus detection software periodically, preferably

automatically without requiring intervention by users.

Require <u>all</u> diskettes and CDs to be checked for viruses. This includes shrink wrapped software as well as preformatted diskettes.

There are numerous reports of shrink-wrapped software and preformatted diskettes being infected with viruses. In addition, employees bringing diskettes from home or other sources may unknowingly transmit a virus. Therefore scan **<u>all</u>** diskettes and CDs brought into the institution, regardless of the source, for viruses before being installed on network-connected desktop systems and network-capable notebook computers.

Use trusted third parties to evaluate network security.

The best security is proactive security. It is far better for an institution to discover network vulnerabilities before these weaknesses are discovered by attackers. There are a number of firms that offer the specialized service of network security assessments that will identify network vulnerabilities. However, monitor the activities of these firms closely, since the "friendly attackers" usually are successful and have the potential to gain access to highly sensitive information and critical business processes. These assessments often include unscheduled network attacks to test the ability of the institution's staff to detect them.

In addition, arrange for a cooperative assessment of network security involving the institution's personnel along with outside experts. Assessments that take advantage of the expert knowledge of the institution's personnel are more likely to uncover systemic security vulnerabilities in a less hostile assessment environment.

As an additional security measure, monitor bulletin boards, chat rooms, and other mechanisms for disseminating information about institutions' security weaknesses, or consider using a trusted third party to provide these services.

Arrange to receive notifications of security vulnerabilities

There are several organizations that are clearing houses for security vulnerabilities in operating systems and application software that are exploited by attackers. These organizations distribute advisories with information about reported security vulnerabilities. These advisories frequently have information about the resolution of the problems they identify. Follow the instructions on these organizations' Web sites to be added to the e-mail distribution list of these advisories; alternatively, use a trusted third party to provide these services.

Inventory and control points of external connectivity to the institution's network.

Points of external connectivity represent potential points where an institution's network can be attacked. Therefore, carefully inventory and control these points of access. Implement all dial-in access to the network via a modem pool protected by a firewall or other security techniques as discussed above.

Particular attention should be given to business-partner connectivity as the business partner's network may provide additional points of entry into an institution's network.

Improve system and network operating system security features wherever possible.

Commercially available security subsystems are available to work with the most widely sold system and network operating systems. These security subsystems can significantly enhance the security of operating systems. For example, the security subsystem will break up the "root" or "superuser" privileges among several system or network administrators, thereby limiting the power and control of any one individual over the system or network. Security subsystems typically also have enhanced auditing capabilities to establish accountability, particularly for system and network administrators.

Personnel

Subject employees with access to sensitive information to rigorous screening procedures.

Carefully screen systems administrators, support personnel, systems programmers and others who are in positions to access sensitive information and/or to have detailed knowledge about security methods and procedures. These procedures should include:

- A thorough background check to ensure that items on the applicant's resume are correct, including educational attainments, previous positions and responsibilities, and outside affiliations.

- A fingerprint check with local and federal authorities to ensure that the applicant has not engaged in criminal activities.

- A thorough and in-depth interview process with the appropriate experts to ensure that the applicant has the technical training and knowledge

claimed on the resume.

- A credit check to ensure that the applicant/employee does not have a questionable credit history or unsustainable debts.

- Drug tests to ensure that the applicant/employee is not using illegal substances.

Subject consultants to the same security checks and screening processes as employees.

Consultants retained for their specialized skills or knowledge may have access to confidential information, or may be in a position to learn about an institution's network topology, access control procedures, and other security vulnerabilities. Therefore, subject consultants to the same rigorous screening process as employees with equivalent access to confidential information. Consultant subcontractors should be similarly screened. Require stringent non-disclosure agreements with consultants and their subcontractors.

Ensure that key technical personnel receive adequate training to become, and to remain, current in their areas of expertise.

Because of rapid technological changes, continuous training of technical personnel in key positions is essential. To stay current, key technical personnel should periodically attend seminars, conferences and training sessions.

Take measures to protect against "social engineering."

One of the more effective means by which attackers gain access to sensitive information is the "low-tech" but effective technique of "social engineering." "Social engineering" is the self-misrepresentation by malicious attackers, for example, as users in distress or help desk personnel troubleshooting a problem. Since help desk personnel are trained to be very helpful, train them in social engineering techniques and have firm policies to follow with regard to providing information that could result in unauthorized access to confidential information. Similarly, train users not to provide information to someone representing himself or herself as a technician or help desk person that could allow that person to gain access to confidential data.

Strongly encourage users to bring anomalous behavior of a network to the attention of a system administrator.

The discovery of attackers is often initiated by users that notice anomalies in their data or their business processes. Encourage users to contact system administrators when unusual situations occur. For example, the unexpected loss of communications with a sensitive database may indicate that the session is being hijacked by an attacker. Provide positive feedback to users who bring anomalies to the attention of systems administrators to encourage their continued vigilance.

Business Continuity

Ensure that contingency back-up sites have the same level of security as primary sites.

Security at contingency back-up sites is frequently less robust than at primary sites. Attackers may cause a failure at a primary site to force operations to be resumed at the less-secure contingency site, creating opportunities for malicious or fraudulent activities. Therefore, it is important to maintain the same level of security at primary and contingency sites.

Ensure that security systems are Year 2000 compliant

Date-sensitive network security systems may be vulnerable to the Year 2000 problem. In order to ensure that serious security problems do not occur at the beginning of the millennium, review, throughly test, and modify if necessary network security systems so that they interpret the year 2000 correctly.

Appendix B

Sound Practices for Internet Security: A Senior Management Perspective

The technology and the terminology of Internet security[7] is evolving at a rapid pace. The objective of this Appendix is to provide a discussion about Internet security in terms that allow senior management to better understand the measures necessary to ensure the security of their organization's Internet site. Initially, the issues associated with Internet security are discussed in terms of functionality to provide a conceptual framework. Some terminology also will be introduced to facilitate the discussion of these issues with technical staff. This Appendix refers to information in "Sound Practices Guidance for Information Security for Networks" and Appendix A, "Sound Practices for Private Local and Wide Area Networks." Similarly, the sound practices in this Appendix are not regulation and should not be interpreted as such.

This Appendix is organized as follows:

- A discussion of Internet security concepts at an overview level;
- An introduction of Internet security terminology;
- A discussion of the security measures appropriate for the three types of Internet sites defined in the body of the paper, and
- A presentation of Internet sound practices.

Management Overview

Much like the servers on institutions' private local and wide area networks that support automated business-related processes, services on Internet sites are provided by servers. Appendix A discussed measures necessary to protect servers on internal networks. The same principles apply to Internet sites; however, because of the exposure of these sites to attacks from the general public via the Internet, the risks associated with these sites are heightened. Similarly, intranets require additional security measures to mitigate the security vulnerabilities

[7]The discussion of Internet security also applies to internal networks that use Internet technology. These networks are known as "intranets."

associated with the non-proprietary Internet technology.

The basic element of Internet-technology security is the "firewall," which provides protection against attacks for Internet sites, internal networks accessible from institutions' Internet sites, and critical intranet network segments. Firewalls, which are discussed in more detail below, may appear at different points in network configurations to protect particularly vulnerable or valuable assets.

"Sound Practices Guidance for Information Security for Networks" discussed three types of Internet sites employed by financial services institutions:

- Information-Only Sites;
- Information-Exchange Sites; and
- Fully Transactional Sites.

All of these sites should be protected by one or more firewalls. In addition, since some implementations of Information-Exchange Sites and Fully Transactional Sites provide a path from the Internet site to the institution's internal network, a firewall should be placed between the site and the internal network to protect the internal network. Similarly, critical intranet network segments should be separated from less critical network segments by firewalls.

The Firewall

A firewall controls access between:

- the Internet and an institution's Internet site;
- an institution's Internet site and internal networks; and
- intranet network segments.

Because of the widely varying definitions of what constitutes a "firewall," this paper will use the term "firewall complex" (see Figure 1) to encompass the following functionalities, which are described in further detail in the next section:

- Address screening -- which ensures delivery of only properly addressed messages and filters-out messages from known troublesome sources.

- Network Isolation -- which logically isolates the Internet site, internal network, or critical segment of an intranet from less secure networks or network segments, and inhibits outsiders from learning about the internal network design.

- Application Screening -- which limits the types of messages that are allowed into internal networks and enables exclusion of file types known to be exploitable by attackers into gaining control of an internal network or damaging and/or reading information on it.

- Message-flow inspection -- which makes a judgment about the appropriateness of any one message in an exchange of related messages between a browser[8] and an Internet-site server. This capability may be appended to one or more of the functionalities described above: address screening, network isolation, or application screening.

These functionalities are incorporated in commercially available versions of "firewalls" in many different forms and configurations.

Introducing Internet-Security Terminology

The following sections discuss the above functionalities in more detail and introduce terminology related to firewall concepts and to the network behind the firewall to facilitate discussions with technical staff. The following firewall functionalities are conceptual; some of them may be combined in software that runs on a single computer.

The Firewall

Address Screening

The device that stops messages with the inappropriate network addresses is usually known as a "screening router." For example, it is supplied with rules to filter out messages from external devices with an internal device's address ("spoofing"[9] attempts) and may also have rules to protect against known sources of attacks.

---

[8] A "browser" is the application on desktop systems that provides Internet access.

[9] See the main body of the paper for a definition of this term.

Network Isolation

The device that isolates the Internet-site, internal network, or intranet segment from less secure networks or network segments is usually known as a "bastion host." The bastion host has an address that is publicly known and all external messages destined for devices behind the bastion host use this address. The bastion host converts the publicly available address to the internal names or addresses of the devices on the protected network, which are kept secret so an attacker will be inhibited from gaining the internal names or addresses.

The bastion host also generates audit trails of all network-related activity. Software called "audit reduction tools" read the audit trails or logs and look for known patterns of inappropriate activity (e.g., multiple attempts to guess a user's password), which result in alerts to the system administrator. These alerts are messages to a system administrator's console and/or a message to the administrator's pager. The use of reduction tools to extract information from these logs is important, because the logs can be extremely large and scanning them manually is so time-consuming it is often avoided. However, in addition to the use of audit reduction tools, the periodic scan of logs by knowledgeable system administrators is invaluable since new patterns of attack may develop that are not recognized by the tools. Also, it is important to kept the bastion host software and audit reduction tool software current, because the updates continually improve security. Also, the audit trails should be stored on a separate server from the bastion host, to keep an intruder from deleting audit trails that would otherwise provide evidence of intrusion.

Application Screening

A device known as a "proxy server" is programmed to administer applications' rules and detect messages with any deviations from or extensions of the applications. The proxy server runs a "proxy" version of the Internet application software. This is to prevent attackers from embedding instructions, or sequences of commands, that will result in the attacker damaging or gaining administrator-level access to the server.

Message-flow Inspection

A problem with Internet technology is that there is inherently no history kept about Internet messages. Each message arrives with essentially no information about preceding or succeeding messages. This makes it difficult to make a judgement about the appropriateness of any one message in a dialog (i.e., an exchange of a series of related messages) between a browser and a Internet-

site server. There is a technology known as "stateful inspection" that addresses this problem by establishing a database of the "state" (history) of each message in a dialog. This allows the "stateful inspection" device to recognize inappropriate responses by a server to messages or inquiries. For example, if a request in a dialog established to provide account information results in a response that incorporates the use of an inappropriate service, such as the transfer of a (possibly confidential) file, "stateful inspection" will recognize that it is an inappropriate response and terminate the session. Stateful inspection technology may be incorporated in one or more of the devices described above: the screening router, bastion host, or proxy server.

The Demilitarized Zone (DMZ)

Traffic from the firewall complex is passed to a small network that is usually known as the "demilitarized zone" (DMZ) since firewall complex provides protection for this network. The servers that supply the site's Internet services are connected to this network. The DMZ usually has at least two elements:

- A device to translate the addresses in the familiar format of the Internet (www.bank.com) to the network addresses of the servers on the DMZ. This is known as the Domain Name Server (DNS).

- The Internet-site server(s).

Domain Name Server (DNS)

The Domain Name Server translates the alphabetic names in the Internet format (www.bank.com) to the internal numeric addresses of the server(s) on the DMZ network. If the site has multiple servers on the network segment for high availability (see below), the DNS can provide "Round Robin" capabilities; that is, the DNS directs incoming messages to first one server and then the next. This provides some protection against denial of service attacks[10] as it can minimize the probability that any one server is flooded by service requests.

Internet-site Server(s)

Finally, there are one or more servers that contain the information and provide the services to the public. High-availability sites require redundant servers,

[10] "Denial of service attacks" are attacks that attempt to overwhelm a server with requests for services from one or more attackers so that the server can not respond to legitimate service requests.

among other measures, so that if one or more of the servers fails, is being serviced, or is attacked, the other servers can provide the site's services.

Protection of Internet Sites

Information-Only Internet Sites

Information-only sites represent the lowest risk to institutions because there is normally no connectivity between the Internet site and the institution's internal network. However, there is significant reputational risk, since the site may be penetrated and inappropriate material or inaccurate information stored on it or it could be used to launch attacks on other Internet sites. These sites may be provided by the institution using its own facilities or by a service provider. In either case, the firewall complex is necessary to minimize the institution's reputational risk. Although the DMZ of an information-only site is usually isolated from a financial service institution's internal network as shown in Figure 1, it is good practice to have only publicly available information on the DMZ to minimize reputational and, possibly, legal risk if the firewall complex is penetrated.

Information-Exchange Sites:

Information-exchange sites (see Figure 2), in addition to supplying information as described above, may function in one or more of the following ways:

- Through the exchange of e-mail.
- Through the submission of forms to a database on a database server connected to the site's server(s) (e.g., loan applications).
- By querying a database on a database server connected to the site's server(s) (account balance information).

E-mail Exchange

Since the exchange of e-mail with external users typically requires a path from the Internet site to the internal network for the distribution of messages to, and receipt of responses from, internal users, additional safeguards beyond the firewall complex are required to protect the internal network. These are described below. For conceptual clarity, the path that e-mail messages take to/from the internal network on the left side of Figure 2 is shown separately from the information flow to/from the site's

servers on the right side of Figure 2. This is not technically required: both e-mail and site servers can be protected by the same firewall complex and can reside on the same DMZ.

The proxy server, which provides the application screening functionality of the firewall complex, in this case runs an e-mail proxy application. The e-mail proxy may check for viruses, or there may be virus protection software running on a server on the DMZ, as shown in Figure 2. This software may "unpack" e-mail attachments (i.e., convert them from the format in which they are written, such as compressed Word or WordPerfect) and screen them for viruses.

There should be an e-mail server on the DMZ to transmit/receive e-mail messages in the Internet e-mail format (known as the Simple Message Transport Protocol, or SMTP). These messages are forwarded to the institution's internal e-mail server for distribution to users. The additional e-mail server on the DMZ provides another layer of protection for the internal network.

There are three more elements in the path to the e-mail server on the institution's internal network:

Protocol[11] *converter*

The protocol converter translates the messages from the communications protocol used by the Internet (TCP/IP) into the communications protocol used by the institution's internal network. (e.g., the X.400 protocol). This has the advantage of placing another obstacle in the path of an attacker.

E-mail gateway

The e-mail gateway converts messages in the Internet's message format (SMTP) to the format of the institution's internal e-mail system. This conversion adds yet another complication for an attacker.

Router[12]

[11] "Protocols" are the agreed-upon rules and formats that define how computers communicate with each other over networks.

[12] "Routers" read the network addresses in messages and forward them to the appropriate network.

A router directs e-mail messages to the internal network, where the institution's e-mail server distributes the messages over the private local or wide area networks.

Although there is a logical path from the Internet to the institutions' internal networks via e-mail, the configuration described above poses sufficient obstacles to an attacker so that an attack can usually be detected and deflected before the internal network is compromised.

Submission of forms and database queries

The right side of Figure 2 shows the path taken by inquiries (e.g., account inquiries) and forms submission (e.g., loan applications) to the database server that supports these functions. Only one server is shown in Figure 2; there may be more than one in a production environment. Inquiries or updates received from users on the Internet are processed by the site servers, which create the structured database queries that are passed to the database server. Responses received from the database server are converted into user-readable messages by the site servers and passed though the firewall complex to the requesting users.

There is no path from the database server to the business-application server on the internal network. This prevents attackers, who may gain control of the database server, from mounting an attack on the internal network. This means that the database server must be manually updated from CDS, diskettes or tapes.

If there is a connection between the database server and the internal network to allow periodic batch updates of the database, the same security measures must be provided as for fully transactional sites, as described below. Even if only briefly established at intervals, the handshake establishing connectivity could be enough to leave a Trojan horse.

Fully Transactional Sites

Fully transactional sites provide the greatest risk to institutions because they typically have a path from the Internet to the institutions' internal networks. In addition to the steps discussed below, it is prudent to take the measures described in Appendix A to protect the internal network, including encryption of highly sensitive data. This ensures that if an attacker does succeed in penetrating to the internal network, there are additional safeguards and obstacles in place to protect highly sensitive data and critical business processes.

As shown in Figure 3, fully transactional sites are protected by the firewall complex and have servers on a DMZ. The difference from an information exchange site is that the database server is separated from the site servers by a firewall complex. This protects the database server and internal network even if an attacker has gained control of the site server(s). The database server communicates with the institution's business-applications interactively (or via batch updates) through a router. Although there is a logical path from the Internet to the institution's internal network, there are sufficient obstacles in attackers' paths to prevent them from penetrating the internal network, or at least slowing them down sufficiently to allow the network administrator to detect the attack and take defensive measures.

Internet Security Sound Practices

Set up an Internet incident response group.

The Internet is a dynamic, risky network environment. Trusted, skilled employees are needed to monitor activities related to Internet connections, respond appropriately to any attack attempts, and report to management as necessary.

Check personnel backgrounds carefully.

Internet security ultimately relies on trusting a small group of skilled employees or an Internet service provider. It is important that due diligence is conducted to minimize risks from untrustworthy persons performing these sensitive functions.

Keep the firewall and site server configurations simple. Implement only the applications, utilities and services required for the firewall or Internet-site server to support the institution's business needs; remove everything else.

Most attacks are based upon known weaknesses in operating systems and/or associated utilities. Therefore, eliminate all services and utilities not directly associated with the functionality of the server or firewall necessary to support business activities.

Properly configure file and directory access controls.

Standard operating systems provide file- and directory-level access controls. Ensure that these are properly configured to inhibit attackers from accessing and modifying critical files or directories. This presents additional

obstacles to attackers that have penetrated the firewall and are attempting to gain access to the site's servers. Ensure that all default accounts are deleted and that all default passwords are changed.

Use commercially available applications to periodically probe networks and firewalls for weaknesses.

Security assessment products are available commercially that assemble "libraries" of attacks based on known weaknesses that can be run against an institution's firewalls and networks. These tools look for administrative and configuration weaknesses as well as security vulnerabilities, such as not changing default passwords. The best security is proactive security: better to learn of weaknesses in your networks and/or firewalls before an attacker does. Run these security assessment tools periodically, particularly after changes have been made to any aspect of the network.

Consider using a separate proxy server for each application.

An additional level of security can be provided by using distributed proxy servers; that is, have a separate proxy server for each application (e.g., web services, file transfers, e-mail, etc.). Although several proxy applications can run on one proxy server, using separate proxy servers for each application has the following advantages:

- Traffic can be better managed by isolating the proxy servers. The demand for each service can be followed by monitoring the traffic through the associated proxy server.

- Separate application proxy servers make it easier to provide high availability, because if one proxy server is disabled the others will continue to operate normally.

- Each proxy server is less complex; therefore, there is less opportunity for error.

Perform due diligence with regard to service providers' security measures and require a comprehensive contract with service providers that covers security issues.

Even though the operation of an Internet site may be outsourced to one or more firms, there continues to be significant reputational risk if the outsourcers' sites are attacked and altered or if the site is used to attack other sites. Therefore,

before entering into a contract with an outsourcer, carefully review the outsourcer's security arrangements. If the necessary expertise is not available in-house, retain an independent security consultant to perform this review. If there is a connection from the institution's internal network to the service provider, ensure that there is a firewall complex protecting the internal network. Institutions using a service provider should make sure that a separate firewall complex protects them, i.e. they are not sharing a firewall complex with another firm.

Provide each desktop system on the network with virus scanning software and/or provide virus scanning software at critical entry points, such as e-mail proxy servers.

Particularly for information-exchange and fully transactional sites that allow customers to send e-mail to individuals or service areas within an institution, the detection of viruses in e-mail attachments is essential. Internet access, if provided to employees, is another potential source of viruses. Virus detection can be done at the entry point (i.e., at the firewall or proxy server), at the desktop, or, preferably, both. It is highly desirable to have virus detection software on each desktop system and on each notebook computer. However, if virus detection is provided only at the entry point, additional awareness training must be given to employees with regard to checking CDS and diskettes for viruses. Update virus detection software periodically, at least every 30 days, preferably without requiring intervention by users (i.e., automatically). Word processor viruses (so-called "macro viruses", because they are embedded in macro programs that give word processors extra functionality) require special virus detection software.

Do not allow any external users to "Telnet" into <u>any</u> critical network components. Allow outgoing Telnet sessions only to specific locations.

"Telnet" is an application that allows remote users to sign on to local servers, thereby raising the risk of these users seizing control of the local device. Therefore, if any employee is allowed to telnet to any critical network component, use strong authentication and encrypted sessions.

Consider the use of public key/private key encryption technology to establish secure communications with customers.

Public/private key encryption, or asymmetric encryption, consists of a key pair: one key is made known as widely as possible; the other is known only to the customer. If an institution receives a message encrypted with a customer's private key, and if the institution is able to decrypt the message using the customer's public key, then the institution knows that the customer originated the

message (unless the customer has lost control of the private key). This is a strong form of authentication. Similarly, if the institution encrypts a message using the customer's public key, ***only*** the customer can decrypt the message with his/her private key. Since symmetric cryptography, where the same key is used to encrypt and decrypt data, is more efficient than public/private key encryption, public/private key encryption is often used to authenticate the customer and to establish secure communications sessions to exchange symmetric keys. Although public/private key management is not fully developed and does not yet scale to wide-spread public implementation, the technology warrants tracking and possible adoption.

Require strong authentication for customers when providing fully transactional processing services.

Knowing with whom one is dealing over the Internet requires strong authentication of the customer. In addition to the techniques discussed in "Sound Practices Guidance for Information Security for Networks," an emerging technology for accomplishing this is the use of digital certificates. Digital certificates consist of information about the holder of the certificate, the certificate-holder's public key, the certificate's expiration date, and the digital signature of the certification authority that issued the certificate. The certification authority may be the institution providing the fully transactional services, or may be a trusted third party. Ideally, the digital certificate is on a smart card held by the user, who is strongly encouraged to maintain physical possession of the smart card at all times and to promptly notify the issuer of the digital certificate if it is lost or stolen. An interim alternative technology is for the digital certificate to reside on the user's hard drive, although it is susceptible to acquisition by an attacker who gains access to the users' desktop system. The technology of digital certificates has not yet demonstrated the capability to scale to wide-spread public implementation, but it also warrants tracking and possible adoption.

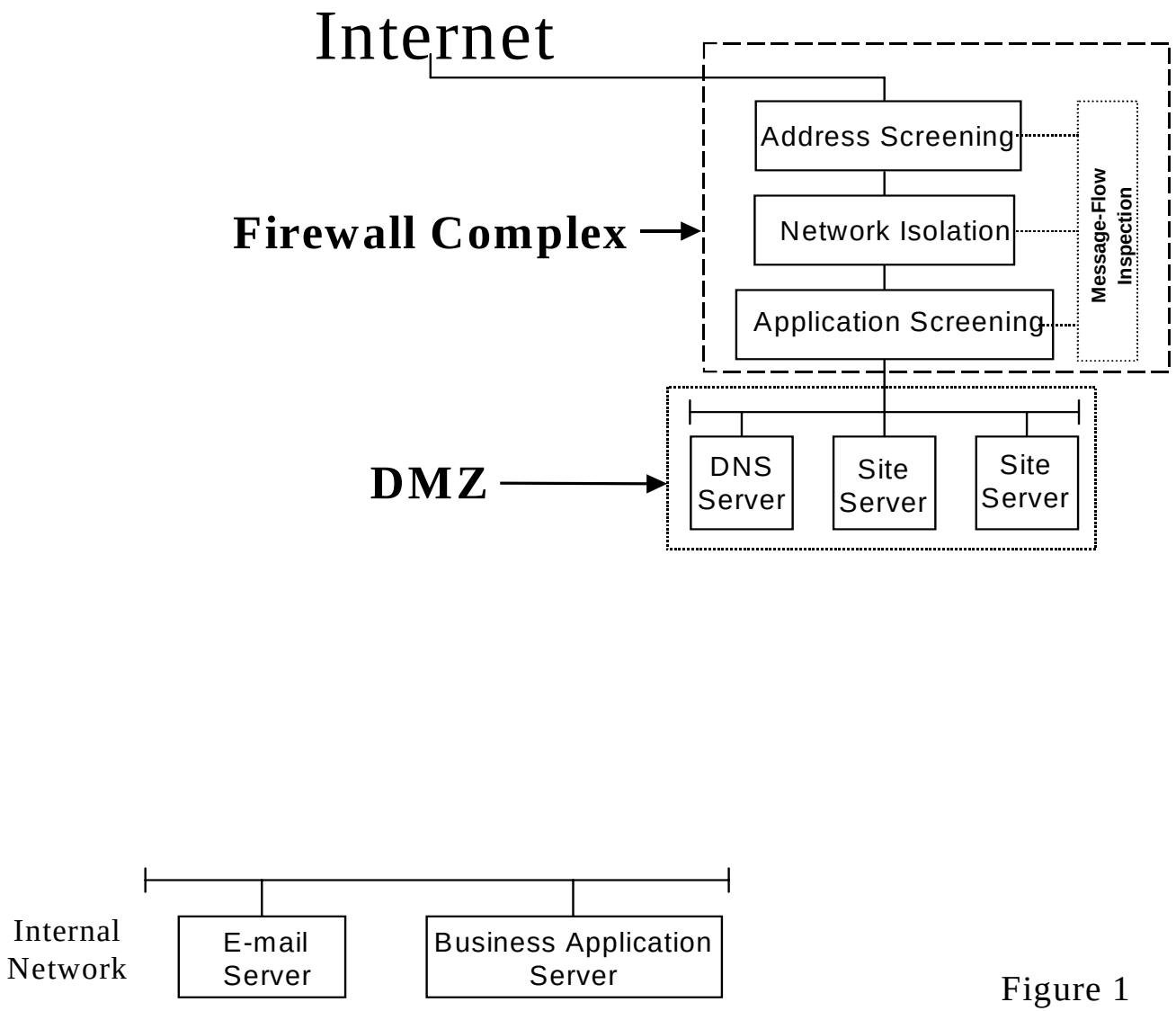
Internet
Firewall Complex
Address Screening
Network Isolation
Application Screening
Message-Flow Inspection
DMZ
DNS Server
Site Server
Site Server
Internal Network
E-mail Server
Business Application Server

Figure 1

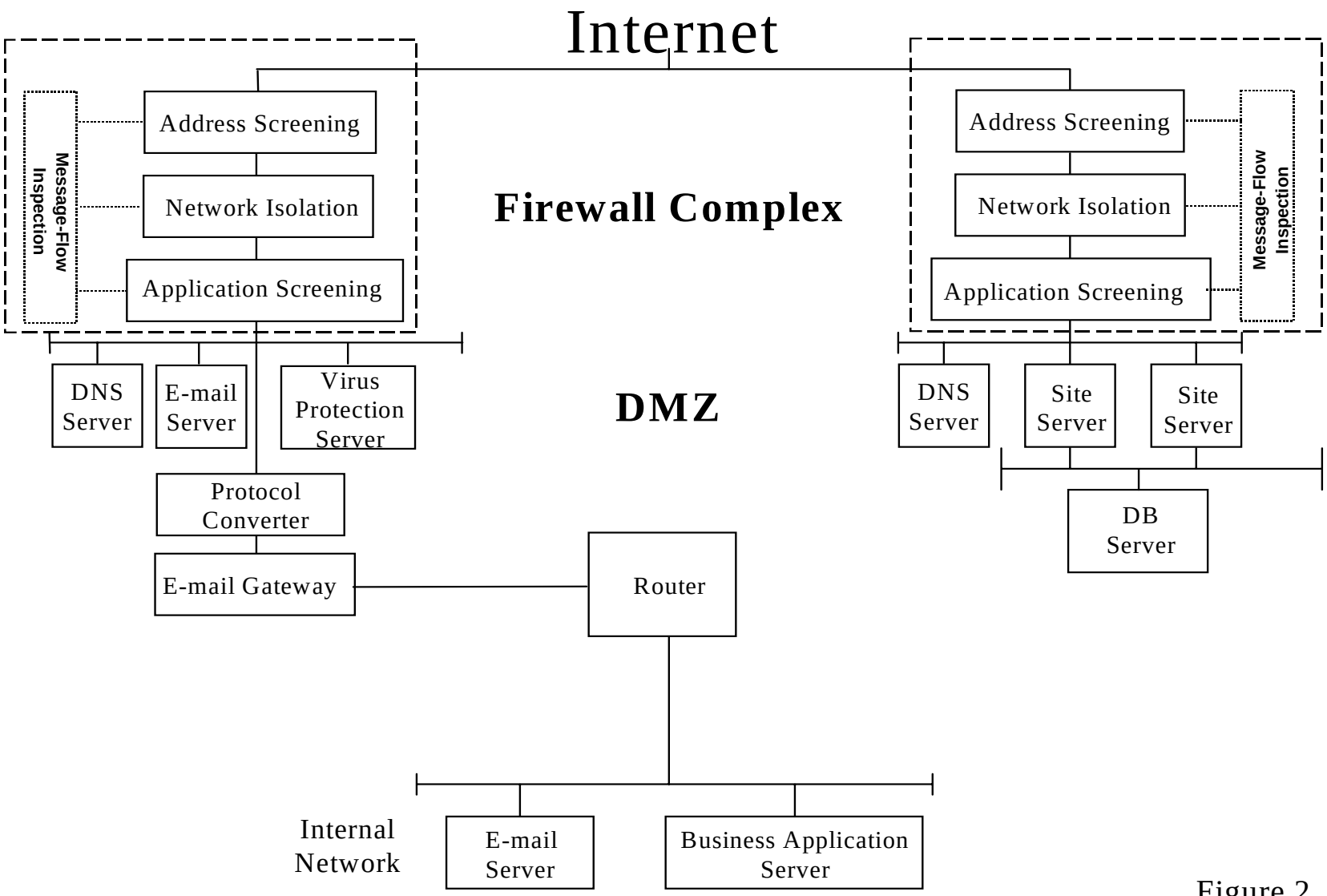
Internet
Address Screening
Network Isolation
Application Screening
Message-Flow Inspection
Firewall Complex
Address Screening
Network Isolation
Application Screening
Message-Flow Inspection
DNS Server
E-mail Server
Virus Protection Server
DMZ
DNS Server
Site Server
Site Server
DB Server
Protocol Converter
E-mail Gateway
Router
Internal Network
E-mail Server
Business Application Server

Figure 2

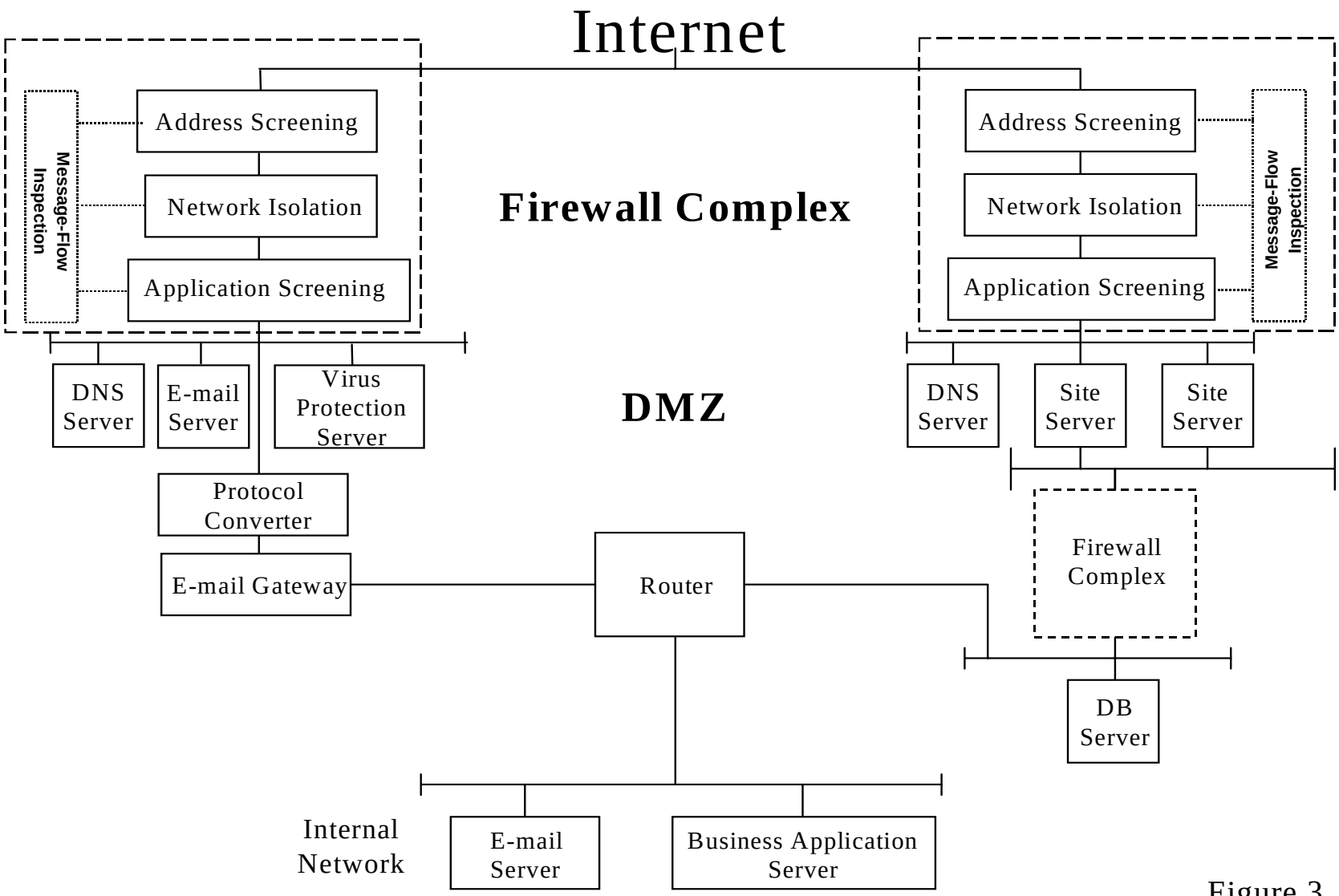
Internet
Address Screening
Network Isolation
Application Screening
Message-Flow Inspection
Firewall Complex
Address Screening
Network Isolation
Application Screening
Message-Flow Inspection
DNS Server
E-mail Server
Virus Protection Server
DMZ
DNS Server
Site Server
Site Server
Protocol Converter
E-mail Gateway
Router
Firewall Complex
DB Server
Internal Network
E-mail Server
Business Application Server

Figure 3