

How to Use This Manual

Computers can increase productivity and efficiency within a financial institution, or they can be used to commit theft and cause substantial financial loss. Computer crime in financial institutions is an increasing concern because computer processing can circumvent traditional security and control techniques.

Most experts believe that computer crime is increasing significantly. Exposure to computer crime is on the rise with the advent of elaborate communications networks, closely coupled computer systems, networks of all sizes, and users who are much more technically sophisticated than the users of previous years.

It is important to recognize that there are two categories of computer crime: discovered and undiscovered. Successful computer crime schemes may still be working well. Many of the criminals have been caught by accident.

Computer fraud is certainly not new and does not necessarily involve the use of computers; they just make it easier. Computer thieves, even if caught, are not prosecuted in many cases. As a result, the problem of white-collar computer crime continues to increase. Many computer fraud cases are never reported because of potential embarrassment to the institution, loss of public confidence, false arrest concerns, and the overall difficulty of prosecution. Many analysts believe that billions of dollars are lost annually to white-collar computer crime.

Traditionally, the time needed for criminal acts is measured in minutes, hours, days, weeks, months, and years. Today, some crimes are being perpetrated in milliseconds because of the speed of the execution of instructions in computers. Also, geographic constraints do not inhibit this new kind of crime. A telephone with a PC attached to it in one part of the world could be used to engage in a crime in a computer system in any other part of the world.

The technologies that underlie network and information security are not only complicated, but also use a jargon of their own that is not common knowledge. The use of three-letter acronyms abound in the area of cryptology and information security.

PURPOSE OF THIS BOOK

This book provides an easy-to-understand process for security planning that focuses on business risks, related threats, tools for addressing the threats, and the processes needed to build more secure systems and continuously monitor and improve security. Several forms, charts, and diagrams are included to facilitate performing the process in a logical and efficient manner.

Information technology (IT) infrastructure security is a complicated subject. Opportunistic attackers routinely exploit security vulnerabilities, which are easily identified and rarely fixed. IT security is usually addressed by experienced security professionals. However, there are an increasing number of people that need to understand the fundamentals of security in a rapidly changing technology world. This

book is written for bank management, IT management, and less experienced security administrators to help them understand and deal with existing security risks. This book can be used as a guide for security “best practices” because it provides a wider perspective on security in general for better understanding how to reduce and manage security risk.

There are no perfect security systems when people are the users of those systems. Technology alone is not enough to build secure business systems. People can undo the most secure of systems by their failure to implement the processes and procedures that accompany the proper use of technology.

Networks continue to grow as organizations migrate from a central to a distributed computing environment. This creates more users in a widespread geographical area. The need to organize and conduct business securely across the enterprise network has become increasingly critical and complex. Distributed processing, global networking, and open architectures have made computer systems easier to use and provide computer access to a wider population. However, this technology significantly complicates the challenge of securing an organization’s information resources. Opportunities for electronic commerce and information exchange are more prevalent and, therefore, security is a critical factor.

The world has been revolutionized by the Internet. Many organizations have addressed globalization issues through the use of the Internet. Business have increased productivity and saved time and money by developing technology that works with their business partners and customers. Businesses are sharing more functions via the Internet to eliminate duplication and to provide economies and efficiencies of scale. However, there is no assurance that information sent over the Internet will arrive at its destination, without being overheard or intercepted. Security tools are available that can reduce the risk in these areas.

SECURITY PLANNING PROCESS

The goal of security planning is to protect the integrity, confidentiality, and availability of information. An effective security plan consists of a cohesive system of resource protection, system monitoring, data collection, and coordinated responses to detected incidents. Securing systems is not a one-time fix. It is an ongoing process that targets a dynamic environment in which new threats arise daily.

A complete security plan should address business information assets as well as the security process. A security plan should be reasonable and practical for the financial institution and may vary, depending on the type of information being protected, the type of business activities being performed, and with whom the business is conducted.

A security plan should address the core business processes throughout the financial institution and requires the support of all the business units. As a result, all business units should be involved in both the initial and continuing planning efforts. Security tends to be a “weak link” problem in that the total security is no better than the weakest point in the organization. Security, therefore, should be evaluated broadly across the entire enterprise to identify and address any weak links.

ORGANIZATION OF THE MANUAL

This manual is organized into six sections that correlate with various phases of the security planning process. Security planning generally consists of the following six contiguous and continuous phases:

- Part I: Risk Assessment Phase
- Part II: Protective Controls Phase
- Part III: Detective Controls Phase
- Part IV: Technology Management Phase
- Part V: Response Management Phase
- Part VI: Compliance Management Phase

These six phases provide for a continuous cycle of refinement and evolution of security. The cycle provides for an assessment of internal and external risks, reasonable and prudent protective measures, constant and consistent monitoring for detection of anomalies (events), the appropriate responses to such anomalies, and a continuous compliance management program. A brief description of each phase of the process and the correlating chapters are presented below.

Part I. Risk Assessment Phase

Chapter 1: Computer Crime Techniques

It is important in assessing risks to understand the various attack methods used by attackers to compromise network security, as well as to understand how some attacks occur. It is also crucial to keep up-to-date on network security issues. Knowledge of both old and new methods of attack is fundamental to combating them. This chapter presents various computer crime statistics and describes several attack types. The forms and variations of attacks are numerous and usually can be grouped into one of the following categories:

- Information gathering
- Unauthorized access
- Disclosure of information
- Denial of service

Chapter 2: Risk Assessment Process

While all risk cannot be avoided, it should be managed and mitigated where possible. An effective risk management program incorporates risk analysis and assessment. Risk analysis identifies and assesses threats and vulnerabilities to an information system, determines acceptable levels of risk, and provides for

appropriate countermeasures. This chapter describes the risk assessment process, including the following activities:

- Systems inventory and definition
- Vulnerability and threat assessment, including both external and internal risks
- Evaluation of controls
- Business analysis and decision
- Communication and monitoring

Chapter 3: Risk Transfer

It is possible to transfer risks that cannot be controlled by acquiring insurance coverage that address the threats. This chapter describes various aspects of risk transfer, such as business interruption insurance and cyber threat insurance. All threats are not automatically covered. The exposures should be identified through the risk analysis, and the policy should be tailored to address these exposures.

Chapter 4: Computer Crime Legislation

The shift to a borderless, incorporeal environment and the increased risk that information will be stolen and transported in electronic form is difficult to address by relying on older laws written to protect physical property. This chapter describes several federal laws that have been developed to address computer crime.

Part II. Protective Controls Phase

The protective controls phase consists of the steps necessary to safeguard information resources. Comprehensive policies and procedures in conjunction with a risk management program can provide the framework for identifying the types of protection needed and where the protective tools should be placed. The components of the protective controls phase include:

- Physical security
- Authentication
- Passwords
- Access security
- Firewalls
- Encryption
- Malicious software

- Application security and controls
- Biometric identification
- Security awareness

Chapter 5: Physical Security

In most circumstances an intruder that has physical access to network cabling, network hardware such as a router, or hosts attached to a network can manage to subvert any other security measures that are in place. As a result, the first and most important aspect of access security and control is good physical security for all computing equipment and network cabling. It is especially important to maintain tight physical security for any host used as a server, because many attacks on networked systems require physical access to servers and/or peripheral devices attached to the servers (tape drives, disk drives, etc.).

Chapter 6: Authentication and Access Security

Extensive measures must be taken for authentication to ensure access to the network and its systems by properly authorized users. Various levels of authentication include something you know (passwords), something you have (tokens), and something you are (biometrics). These levels provide increasingly stronger assurances as to the identity of the user.

Chapter 7: Passwords

Passwords can be a pervasive aspect of computer security. Although password security may be the most common technique available today, it can be the weakest link in maintaining system integrity. Traditional passwords are problematic because they can be:

- Misused and mismanaged by individuals
- Observed in use
- Tapped from unsecured lines
- Simulated by another computer
- Guessed
- Traded or loaned
- Stolen
- Forgotten

Chapter 8: Operating System Security

Operating system security includes the policies, procedures, and tools that control access to resources. Logical access controls typically are in the form of system user profiles for access to network resources.

Chapter 9: Firewalls

Firewalls are access control tools designed to provide access control protection between trusted networks (corporate) and untrusted networks. A firewall is a system designed to control access to applications on a network — typically access to a private network from the public Internet. Firewalls are needed for several reasons, including:

- Potential loss of mission critical business information
- Potential loss of services such as e-mail, HTTP, FTP, and EDI
- Protection of legal and confidential information
- Prevention of exposure to network servers and workstations
- Enforcement of security policies

Chapter 10: Encryption Techniques

The integrity of data in storage and in transit can be protected through encryption and the use of digital certificates. Encryption scrambles the data to make it unreadable to unauthorized viewers. Digital certificates can be used to verify the sender of the data in transit and to provide assurance that the data was not tampered with during transit.

Chapter 11: Malicious Software

Computer viruses are computer programs that also have the capability to attach themselves to other programs and reproduce and, under certain circumstances, can damage computer systems, data, and programs. While a virus can be benign and cause no harm, many viruses are destructive in nature. A virus may also be dormant for a period of time until it becomes activated.

Chapter 12: Application Security and Controls

Application controls are security techniques unique to a specific computer application system, such as deposit systems, payroll, and various loan systems. Application controls are classified as:

- Application security
- Input controls
- Processing controls
- Output controls

Chapter 12A: Computer Security Logs and Audit Trails

The purpose of this chapter is to provide assistance for organizations in understanding the need for sound computer security log management and audit trails. It provides practical, real-world guidance on

developing, implementing, and maintaining effective security log management and audit trail practices throughout a bank. This chapter is structured into the following major sections:

- Introduction to computer security log management and audit trails, including an explanation of log management needs a bank might have and the challenges involved in log management.
- Description of the components, architectures, and functions of log management infrastructures.
- Explanation of the processes that a bank should develop for organization-level and system-level log management and audit trails, respectively.
- Description of log management-related policy, roles, and responsibilities.

Chapter 13: Biometric Identification

The need for performing financial transactions in complex computer networks over great distances creates a special concern for higher security levels and improved identification techniques. Biometric identification technologies have been developed to increase the probability of positive personal identification.

Chapter 14: Security Awareness

Security awareness programs are designed to educate users on the security policies of an organization. A security awareness program should not only educate about the organization's security policies, but it should also help to foster an understanding of how the policy protects the business, the employees, and customers. Security awareness training should educate high-level employees how monitoring tools are used and what information can be gathered by those tools.

Part III. Detective Controls Phase

Detection should be considered as important as protection. Even the most comprehensive security systems may not protect against all attempts to compromise security measures. The detection phase provides for constant and consistent monitoring for inappropriate system activity and adherence to policies. The multi-phase approach provides for detection of intrusions at network access points, intrusions or misuse of critical systems, and analysis of system policies and procedures. Audit trails provide additional sources for identifying events and provide historical records of such activity. Components of the detection phase include:

- Security administration
- Security policies
- Intrusion detection
- Vulnerability testing

Chapter 15: Security Administration

The security of a computer system involves safeguards for hardware, software, and the data stored within the system. This also involves protecting stored data and preventing unauthorized access and alteration of the stored information. To best administer security within an organization, a security function should be established that oversees a coordinated security program. The security administrator should report to top management so that policies and procedures can be set with proper authority.

Good security begins as an attitude and is carried forward by action and reaction. Security awareness starts at the top of the organizational chart. Management should have a clear understanding of potential exposures to the organization if poor security measures are allowed to exist. Management should take the initiative and develop formal security policies, procedures, and a security awareness program, which can be the vehicle for communicating security policies and procedures to current and new employees.

Chapter 16: Security Policies

End-users must be aware of the threats to the network and its resources and assist in taking protective measures. Written information security policies and the determination of acceptable behavior is paramount to an effective security plan and establishes an enforceable set of rules. Security policies should be reviewed and updated as necessary.

Chapter 17: Intrusion Detection Systems

Intrusion detection systems help computer systems prepare for and deal with attacks. They accomplish this by collecting information from a variety of system and network sources, then analyzing the information for symptoms of security problems. In some cases, intrusion detection systems allow the user to specify real-time responses to security violations. Intrusion detection systems perform a variety of functions, including:

- Monitoring and analysis of user and system activity
- Auditing system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Recognizing activity patterns reflecting known attacks
- Statistical analysis for abnormal activity patterns
- Operating system audit trail management, with recognition of user activity reflecting policy violations

Chapter 17A: Forensic Techniques

Forensic science is generally defined as the application of science to the law. Traditionally, computer data analysis has been associated with data on a computer's storage media, while network data analysis has been associated with data passing through a network. As analysis tools and techniques mature, the two

disciplines intertwine. A combined computer and network data analysis capability is increasingly important for incident handling and operational support.

Chapter 18: Vulnerability Assessment

Vulnerability-assessment products (also known as scanners) are security management tools that:

- Conduct exhaustive checks of systems in an attempt to locate exposures to security vulnerabilities.
- Report the number, nature, and severity of these exposures.
- Allow a system administrator to determine the security status of a system at a particular time.
- Allow security auditors to determine the effectiveness of an organization's system security administration.
- In some cases, once an incident occurs, allow investigators to determine the avenue of entry for an intruder or attacker.

Vulnerability assessment products complement intrusion-detection systems by helping system administrators to be proactive in securing their systems by finding and closing security holes before attackers can use them. Intrusion-detection systems are by nature reactive. They monitor for attackers targeting systems in hopes of interrupting the attacks before the system is damaged.

Part IV. Technology Management Phase

Chapter 19: Organizational Controls

A well-planned and properly functioning organization is an important factor in any system of internal control and in reducing the organization's exposure to the risk of computer crime. The organization structure establishes a framework within which the IT department functions and determines the relationship of the IT department to the rest of the organization. An effective organization structure should provide for segregation of functions and responsibilities so that no one person has duties that would permit the preparation and concealment of material errors or irregularities. Management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management.

Chapter 20: Systems Development and Maintenance Controls

Standards and procedures for systems development and maintenance provide a cornerstone for the continuity of internal control. Systems development and maintenance controls specifically cover two areas:

- Review, testing, and approval of new systems
- Control over program changes to existing systems

These controls are designed to ensure that effective application controls are included in all new systems and to maintain the integrity of programs in production status.

Chapter 21: Systems Development Life Cycle

A systems development life cycle (SDLC) methodology is a structured approach for systems development, from systems planning and design through implementation and support. A methodology is a proven series of steps and tasks systems developers can follow to build quality systems faster, at lower costs, and with less risk. The bank should use industry-accepted design, development, and support techniques and automated management and development tools in implementing a comprehensive SDLC methodology.

Chapter 22: Third-Party Service Organizations

Due to the increasing costs of IT, some financial institutions have found that outsourcing some of their IT functions is more cost beneficial. This has led to the formation of the Application Service Providers and Hosting Service Organization. A third party IT service organization is a technology that manages and delivers application capabilities to multiple entities from a data center across a wide area network (WAN).

Chapter 23: Technology Planning

Technology planning is the process of establishing goals and objectives, defining strategies and policies to achieve these objectives, and developing detailed plans to ensure that the strategies are implemented. Security and controls should be a major consideration in developing the technology plan. The technology planning process is an organizational control that management uses to control the planning and budgeting of technology expenditures.

The need for comprehensive technology planning is increasingly evident. Improved management information has become critical to the effective and efficient management of bank operations. Increased external and internal reporting requirements have heightened the need for more comprehensive management information. Information systems and technology can help to satisfy information needs in a cost-effective manner. But because information systems and technology resources are limited, banks need a plan to optimize technology expenditures.

Chapter 23A: Enterprise Information Technology Security Planning

The purpose of this chapter is to describe a process for security planning and managing risk to organizational operations and assets, individuals, other organizations resulting from the operation and use of information systems. The information provided in this chapter has been broadly developed from a technical perspective to be generally useful across a wide range of organizations employing information systems to implement mission and business processes.

Chapter 23B: Information Security Metrics

Performance metrics can be used as management tools in their internal improvement efforts and link implementation of their information security programs to strategic planning efforts. Information security metrics are used to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. They provide the means for tying

the implementation, efficiency, and effectiveness of security controls to an organization's success in its mission-critical activities. The performance metrics development process described in this chapter will assist information security practitioners in establishing a relationship between information system and program security activities under their purview and the bank mission, helping to demonstrate the value of information security to their bank.

Part V. Response Management Phase

The response management phase is triggered by detection of an anomaly or "event." An automatic event alert should occur based on inappropriate activity and identified attack signature or patterns. Incident response procedures indicate the action to be taken during and after an event occurs. Technical staff should be trained on these procedures to provide for an appropriate and measured response. Response procedures may require the collection and preservation of evidence (forensics) that may be necessary in the advent of an investigation or prosecution. Assessment of events and responses to them can help to refine all phases of the security plan. Disaster recovery procedures may need to be activated, depending upon the severity of the event. Major components of the response management include:

- Incident response and assessment
- Backup and off-site storage
- Disaster recovery

Chapter 24: Incident Response Team

This chapter describes the process for creating an incident response team (IRT). The IRT is a specialized group of internal and/or external people whose responsibility is specifically to manage security-related incidents. The IRT should be composed of individuals with different areas of expertise. When an incident occurs, team members with the appropriate expertise should handle the investigation.

Chapter 25: Incident Response Procedures

Effective procedures are extremely important in an IRT plan. Considerable effort and time are necessary to develop the detailed procedures. However, procedures can be difficult to use and become outdated quickly. Poorly written IRT procedures can be extremely frustrating. Well-written procedures reduce the time required to read and understand the procedures, and therefore, result in a better chance of success of rapid containment and resolution of a security incident. This chapter describes various IRT procedures related to:

- Determination
- Notification
- Containment
- Assessment
- Eradication

- Recovery

Chapter 26: Backup and Off-Site Storage

Backup and off-site storage and protection of vital records is an important aspect of security planning. Most security plans assume that off-site storage will survive. Accordingly, the security planning team should carefully evaluate the safety and soundness of the off-site storage facility. Periodic, regular backups and off-site storage of critical system and database files are an important layer of protection against user error, the most common cause of data loss, as well as extra insurance against threats such as malicious damage caused by disgruntled users, hackers, and malicious code.

Chapter 27: Business Continuity

Business continuity procedures may be activated if the event is severe enough to require them, such as the destruction of a critical system through an intentional or unintentional compromise. It may also happen as the result of a natural disaster.

Part VI. Compliance Management

Computer systems in banking are complex, and the degree of integration between systems adds to this complexity. A variety of platforms are in use and interconnected in an enterprise WAN. Because of this complexity, IT audits should be performed on a periodic basis. An audit and compliance function can provide a reliable method for subjecting these computer systems and their related resources to routine independent review. This will help ensure that control risk is minimized and that IT management is accountable for a proper security and controls environment. IT auditing program and resources can include external auditors, internal auditors, regulatory examiners, and various combinations.

Chapter 28: External Audit

This chapter describes important aspects of the external audit process as it related to security and internal controls. The following major topics are discussed:

- Financial auditing
- Services auditor's reports (SAS No. 70)
- Internal control considerations (SAS No. 94)
- ISO standards

Chapter 29: Internal IT Audit

This chapter explains the need for internal auditing of the IT function. IT auditing should be performed to ensure that:

- Records are being processed accurately in a safe and sound manner.
- Computer-generated information, which management uses for decision making, is reliable.

- Operating procedures are effective and efficient.
- Employees are complying with organizational policies and procedures; regulatory laws, rulings and procedures; and other guidelines, especially in the areas of security, privacy, and confidentiality.
- Unauthorized activities that may compromise the security and integrity of the system are detected.
- The organizational structure provides for the segregation of incompatible responsibilities, such as input, processing, and output as well as the internal accounting controls of authorization, record, and custody.
- Procedures are in effect to assure continuity of services, both from an operational perspective as well as a technical perspective.

IT audits have several benefits. By strengthening internal controls, management can reduce internal control risks and improve the safeguard over assets. IT audits provide management with a means of supplying objective analysis, appraisals, recommendations, counsel, and information the organization's controls and performance.

Chapter 30: Regulatory Agencies

The federal regulatory agencies have an important role in assuring that financial institutions have adequate security and controls. This chapter contains a brief description of the member agencies of the Federal Financial Institutions Examination Council (FFIEC) and relevant sections of the FFIEC Information Security Examination Handbook pertaining to security and controls.

Chapter 31: Computer-Assisted Audit Techniques

The IT audit function should also include security and statistical analysis tools to evaluate the database, such as computer-assisted audit techniques. These tools provide audit efficiencies to verify the integrity of individual systems and to test for compliance with existing system and security policies and procedures. This chapter describes several techniques and provides many examples of the use of such tools to streamline the audit process.

Chapter 32: Laws, Standards, and Guidelines

This chapter contains a brief description of legislation, rules, and directives applicable to information security, including the Health Insurance Portability and Accountability Act.

Chapter 33: Identity Theft Program

This chapter describes various identity theft concerns for banks. It also provides best practices and details related federal laws. The chapter also features several exhibits that discuss consumer considerations related to identity theft, including how consumers can protect themselves.

Chapter 34: Homeland Security

This chapter provides an overview of the new Cabinet-level Department of Homeland Security, including a description of its structure, its area of responsibility, its alert system, and the National Strategy to Secure Cyberspace.

Chapter 35: Spam E-Mail

This chapter discusses the problem of spam e-mail, providing an overview of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, and offering different methods to deal with spam — from both a recipient's and a marketer's point of view.

Part VII. Working Materials

This section is designed to provide your bank with materials that can assist with the security-planning process. Current documents include the following risk assessment worksheets:

Technical Considerations:

- Application controls
- Business continuity planning
- Communications controls
- Computer operations
- Computer room security
- Data backup procedures
- E-commerce security
- Main computer security
- Network security
- Off-site storage
- Program development

Physical Considerations:

- Facility security
- Intrusion detection system
- Key and lock control
- Personnel

- Vital records

Part VIII. Glossary

The final section defines commonly used security and technology terms.