National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

An Introduction to Computer Security: The NIST Handbook

Special Publication 800-12

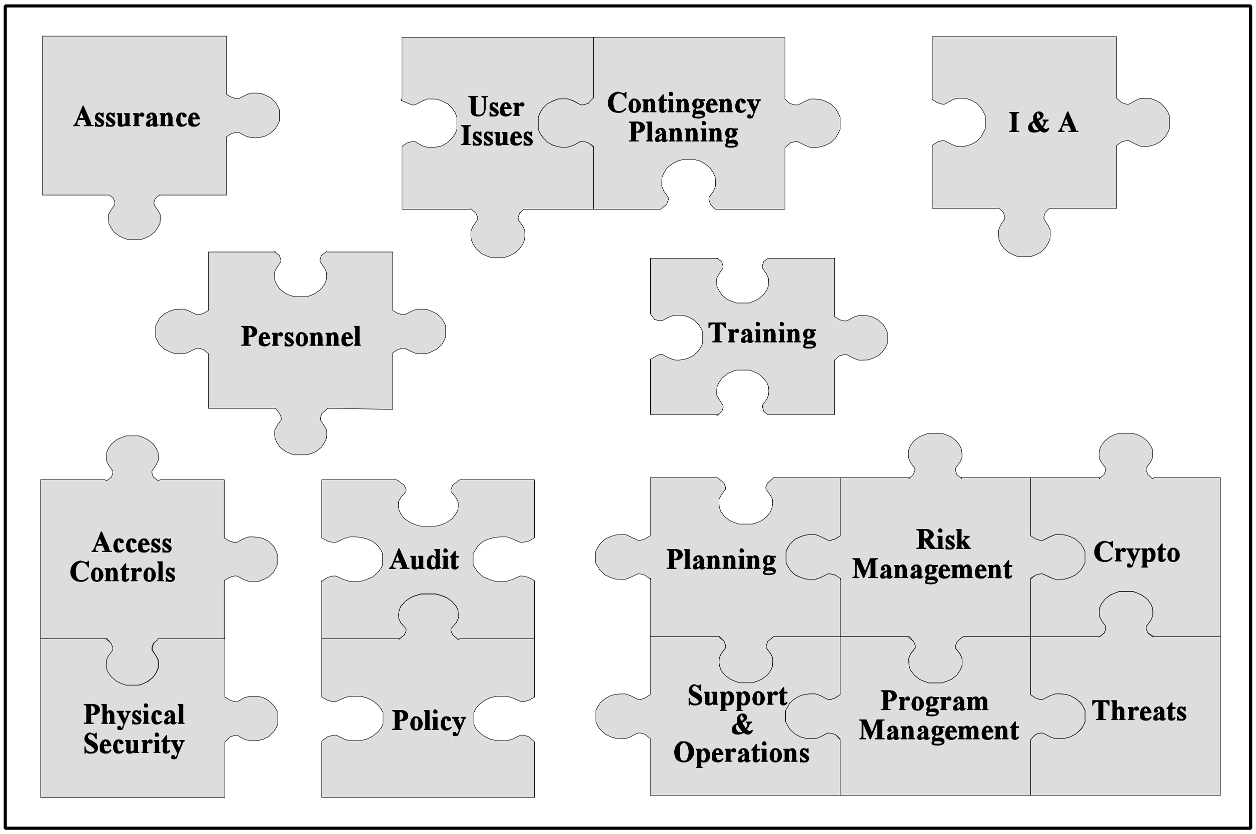

Table of Contents

I. INTRODUCTION AND OVERVIEW

Chapter 1

INTRODUCTION

1.1 Purpose 3
1.2 Intended Audience 3
1.3 Organization 4
1.4 Important Terminology 5
1.5 Legal Foundation for Federal Computer Security Programs 7

Chapter 2

ELEMENTS OF COMPUTER SECURITY

2.1 Computer Security Supports the Mission of the Organization. 9
2.2 Computer Security is an Integral Element of Sound Management. 10
2.3 Computer Security Should Be Cost-Effective. 11
2.4 Computer Security Responsibilities and Accountability Should Be Made Explicit. 12
2.5 Systems Owners Have Security Responsibilities Outside Their Own Organizations. 12
2.6 Computer Security Requires a Comprehensive and Integrated Approach. 13
2.7 Computer Security Should Be Periodically Reassessed. 13
2.8 Computer Security is Constrained by Societal Factors. 14

Chapter 3

ROLES AND RESPONSIBILITIES

3.1 Senior Management 16
3.2 Computer Security Management 16
3.3 Program and Functional Managers/Application Owners 16
3.4 Technology Providers 16
3.5 Supporting Functions 18
3.6 Users 20

Chapter 4

COMMON THREATS: A BRIEF OVERVIEW

4.1 Errors and Omissions 22
4.2 Fraud and Theft 23
4.3 Employee Sabotage 24
4.4 Loss of Physical and Infrastructure Support 24
4.5 Malicious Hackers 24
4.6 Industrial Espionage 26
4.7 Malicious Code 27
4.8 Foreign Government Espionage 27
4.9 Threats to Personal Privacy 28

II. MANAGEMENT CONTROLS

Chapter 5

COMPUTER SECURITY POLICY

5.1 Program Policy 35
5.2 Issue-Specific Policy 37
5.3 System-Specific Policy 40
5.4 Interdependencies 42
5.5 Cost Considerations 43

Chapter 6

COMPUTER SECURITY PROGRAM MANAGEMENT

6.1 Structure of a Computer Security Program 45
6.2 Central Computer Security Programs 47
6.3 Elements of an Effective Central Computer Security Program 51
6.4 System-Level Computer Security Programs 53
6.5 Elements of Effective System-Level Programs 53
6.6 Central and System-Level Program Interactions 56
6.7 Interdependencies 56
6.8 Cost Considerations 56

Chapter 7

COMPUTER SECURITY RISK MANAGEMENT

7.1 Risk Assessment 59
7.2 Risk Mitigation 63
7.3 Uncertainty Analysis 67
7.4 Interdependencies 68
7.5 Cost Considerations 68

Chapter 8

SECURITY AND PLANNING IN THE COMPUTER SYSTEM LIFE CYCLE

8.1 Computer Security Act Issues for Federal Systems 71
8.2 Benefits of Integrating Security in the Computer System Life Cycle 72
8.3 Overview of the Computer System Life Cycle 73

8.4 Security Activities in the Computer System Life Cycle 74
8.5 Interdependencies 86
8.6 Cost Considerations 86

Chapter 9

ASSURANCE

9.1 Accreditation and Assurance 90
9.2 Planning and Assurance 92
9.3 Design and Implementation Assurance 92
9.4 Operational Assurance 96
9.5 Interdependencies 101
9.6 Cost Considerations 101

III. OPERATIONAL CONTROLS

Chapter 10

PERSONNEL/USER ISSUES

10.1 Staffing 107
10.2 User Administration 110
10.3 Contractor Access Considerations 116
10.4 Public Access Considerations 116
10.5 Interdependencies 117
10.6 Cost Considerations 117

Chapter 11

PREPARING FOR CONTINGENCIES AND DISASTERS

11.1 Step 1: Identifying the Mission- or Business-Critical Functions 120

11.2 Step 2: Identifying the Resources That Support Critical Functions . . . 120
11.3 Step 3: Anticipating Potential Contingencies or Disasters . . . 122
11.4 Step 4: Selecting Contingency Planning Strategies . . . 123
11.5 Step 5: Implementing the Contingency Strategies . . . 126
11.6 Step 6: Testing and Revising . . . 128
11.7 Interdependencies . . . 129
11.8 Cost Considerations . . . 129

Chapter 12

COMPUTER SECURITY INCIDENT HANDLING

12.1 Benefits of an Incident Handling Capability . . . 134
12.2 Characteristics of a Successful Incident Handling Capability . . . 137
12.3 Technical Support for Incident Handling . . . 139
12.4 Interdependencies . . . 140
12.5 Cost Considerations . . . 141

Chapter 13

AWARENESS, TRAINING, AND EDUCATION

13.1 Behavior . . . 143
13.2 Accountability . . . 144
13.3 Awareness . . . 144
13.4 Training . . . 146
13.5 Education . . . 147
13.6 Implementation . . . 148
13.7 Interdependencies . . . 152
13.8 Cost Considerations . . . 152

Chapter 14

SECURITY CONSIDERATIONS
IN
COMPUTER SUPPORT AND OPERATIONS

14.1 User Support 156
14.2 Software Support 157
14.3 Configuration Management 157
14.4 Backups 158
14.5 Media Controls 158
14.6 Documentation 161
14.7 Maintenance 161
14.8 Interdependencies 162
14.9 Cost Considerations 163

Chapter 15

PHYSICAL AND ENVIRONMENTAL SECURITY

15.1 Physical Access Controls 166
15.2 Fire Safety Factors 168
15.3 Failure of Supporting Utilities 170
15.4 Structural Collapse 170
15.5 Plumbing Leaks 171
15.6 Interception of Data 171
15.7 Mobile and Portable Systems 172
15.8 Approach to Implementation 172
15.9 Interdependencies 174
15.10 Cost Considerations 174

IV. TECHNICAL CONTROLS

Chapter 16

IDENTIFICATION AND AUTHENTICATION

16.1 I&A Based on Something the User Knows 180
16.2 I&A Based on Something the User Possesses 182
16.3 I&A Based on Something the User Is 186
16.4 Implementing I&A Systems 187
16.5 Interdependencies 189
16.6 Cost Considerations 189

Chapter 17

LOGICAL ACCESS CONTROL

17.1 Access Criteria 194
17.2 Policy: The Impetus for Access Controls 197
17.3 Technical Implementation Mechanisms 198
17.4 Administration of Access Controls 204
17.5 Coordinating Access Controls 206
17.6 Interdependencies 206
17.7 Cost Considerations 207

Chapter 18

AUDIT TRAILS

18.1 Benefits and Objectives 211
18.2 Audit Trails and Logs 214
18.3 Implementation Issues 217
18.4 Interdependencies 220
18.5 Cost Considerations 221

Chapter 19

CRYPTOGRAPHY

19.1 Basic Cryptographic Technologies 223
19.2 Uses of Cryptography 226
19.3 Implementation Issues 230
19.4 Interdependencies 233
19.5 Cost Considerations 234

V. EXAMPLE

Chapter 20

ASSESSING AND MITIGATING THE RISKS TO A HYPOTHETICAL COMPUTER SYSTEM

20.1 Initiating the Risk Assessment 241
20.2 HGA's Computer System 242
20.3 Threats to HGA's Assets 245
20.4 Current Security Measures 248
20.5 Vulnerabilities Reported by the Risk Assessment Team 257
20.6 Recommendations for Mitigating the Identified Vulnerabilities 261
20.7 Summary 266

Cross Reference and General Index 269

Acknowledgments

NIST would like to thank the many people who assisted with the development of this handbook. For their initial recommendation that NIST produce a handbook, we thank the members of the Computer System Security and Privacy Advisory Board, in particular, Robert Courtney, Jr. NIST management officials who supported this effort include: James Burrows, F. Lynn McNulty, Stuart Katzke, Irene Gilbert, and Dennis Steinauer.

In addition, special thanks is due those contractors who helped craft the handbook, prepare drafts, teach classes, and review material:

> Daniel F. Sterne of Trusted Information Systems (TIS, Glenwood, Maryland) served as Project Manager for Trusted Information Systems on this project. In addition, many TIS employees contributed to the handbook, including: David M. Balenson, Martha A. Branstad, Lisa M. Jaworski, Theodore M.P. Lee, Charles P. Pfleeger, Sharon P. Osuna, Diann K. Vechery, Kenneth M. Walker, and Thomas J. Winkler-Parenty.

Additional drafters of handbook chapters include:

> Lawrence Bassham III (NIST), Robert V. Jacobson, International Security Technology, Inc. (New York, NY) and John Wack (NIST).

Significant assistance was also received from:

> Lisa Carnahan (NIST), James Dray (NIST), Donna Dodson (NIST), the Department of Energy, Irene Gilbert (NIST), Elizabeth Greer (NIST), Lawrence Keys (NIST), Elizabeth Lennon (NIST), Joan O'Callaghan (Bethesda, Maryland), Dennis Steinauer (NIST), Kibbie Streetman (Oak Ridge National Laboratory), and the Tennessee Valley Authority.

Moreover, thanks is extended to the reviewers of draft chapters. While many people assisted, the following two individuals were especially tireless:

> Robert Courtney, Jr. (RCI) and Steve Lipner (MITRE and TIS).

Other important contributions and comments were received from:

> Members of the Computer System Security and Privacy Advisory Board, and the Steering Committee of the Federal Computer Security Program Managers' Forum.

Finally, although space does not allow specific acknowledgement of all the individuals who contributed to this effort, their assistance was critical to the preparation of this document.

I. INTRODUCTION AND OVERVIEW

Chapter 1

INTRODUCTION

1.1 Purpose

This handbook provides assistance in securing computer-based resources (including hardware, software, and information) by explaining important concepts, cost considerations, and interrelationships of security controls. It illustrates the benefits of security controls, the major techniques or approaches for each control, and important related considerations.[1]

The handbook provides a broad overview of computer security to help readers understand their computer security needs and develop a sound approach to the selection of appropriate security controls. It does not describe detailed steps necessary to implement a computer security program, provide detailed implementation procedures for security controls, or give guidance for auditing the security of specific systems. General references are provided at the end of this chapter, and references of "how-to" books and articles are provided at the end of each chapter in Parts II, III and IV.

The purpose of this handbook is not to specify requirements but, rather, to discuss the benefits of various computer security controls and situations in which their application may be appropriate. Some requirements for federal systems[2] are noted in the text. This document provides advice and guidance; no penalties are stipulated.

1.2 Intended Audience

The handbook was written primarily for those who have computer security responsibilities and need assistance understanding basic concepts and techniques. Within the federal government,[3] this includes those who have computer security responsibilities for *sensitive* systems.

---

[1] It is recognized that the computer security field continues to evolve. To address changes and new issues, NIST's Computer Systems Laboratory publishes the *CSL Bulletin* series. Those bulletins which deal with security issues can be thought of as supplements to this publication.

[2] Note that these requirements do not arise from this handbook, but from other sources, such as the Computer Security Act of 1987.

[3] In the Computer Security Act of 1987, Congress assigned responsibility to NIST for the preparation of standards and guidelines for the security of sensitive *federal* systems, excluding classified and "Warner Amendment" systems (unclassified intelligence-related), as specified in 10 USC 2315 and 44 USC 3502(2).

For the most part, the concepts presented in the handbook are also applicable to the private sector.[4] While there are differences between federal and private-sector computing, especially in terms of priorities and legal constraints, the underlying principles of computer security and the available safeguards – managerial, operational, and technical – are the same. The handbook is therefore useful to anyone who needs to learn the basics of computer security or wants a broad overview of the subject. However, it is probably too detailed to be employed as a user awareness guide, and is not intended to be used as an audit guide.

Definition of Sensitive Information

Many people think that sensitive information only requires protection from unauthorized disclosure. However, the Computer Security Act provides a much broader definition of the term "sensitive" information:

any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

The above definition can be contrasted with the long-standing confidentiality-based information classification system for national security information (i.e., CONFIDENTIAL, SECRET, and TOP SECRET). This system is based only upon the need to protect classified information from unauthorized disclosure; the U.S. Government does not have a similar system for unclassified information. No governmentwide schemes (for either classified or unclassified information) exist which are based on the need to protect the integrity or availability of information.

1.3 Organization

The first section of the handbook contains background and overview material, briefly discusses of threats, and explains the roles and responsibilities of individuals and organizations involved in computer security. It explains the executive principles of computer security that are used throughout the handbook. For example, one important principle that is repeatedly stressed is that only security measures that are cost-effective should be implemented. A familiarity with the principles is fundamental to understanding the handbook's philosophical approach to the issue of security.

The next three major sections deal with security controls: Management Controls[5] (II), Operational Controls (III), and Technical Controls (IV). Most controls cross the boundaries between management, operational, and technical. Each chapter in the three sections provides a basic explanation of the control; approaches to implementing the control, some cost considerations in selecting, implementing, and using the control; and selected interdependencies that may exist with other controls. Each chapter in this portion of the handbook also provides references that may be useful in actual implementation.

---

[4] As necessary, issues that are specific to the federal environment are noted as such.

[5] The term *management controls* is used in a broad sense and encompasses areas that do not fit neatly into operational or technical controls.

- The *Management Controls* section addresses security topics that can be characterized as managerial. They are techniques and concerns that are normally addressed by management in the organization's computer security program. In general, they focus on the management of the computer security program and the management of risk within the organization.

- The *Operational Controls* section addresses security controls that focus on controls that are, broadly speaking, implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise – and often rely upon management activities as well as technical controls.

- The *Technical Controls* section focuses on security controls that the computer system executes. These controls are dependent upon the proper functioning of the system for their effectiveness. The implementation of technical controls, however, always requires significant operational considerations – and should be consistent with the management of security within the organization.

Finally, an example is presented to aid the reader in correlating some of the major topics discussed in the handbook. It describes a hypothetical system and discusses some of the controls that have been implemented to protect it. This section helps the reader better understand the decisions that must be made in securing a system, and illustrates the interrelationships among controls.

1.4 Important Terminology

To understand the rest of the handbook, the reader must be familiar with the following key terms and definitions as used in this handbook. In the handbook, the terms *computers* and *computer systems* are used to refer to the entire spectrum of information technology, including application and support systems. Other key terms include:

Computer Security: The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Integrity: In lay usage, information has integrity when it is timely, accurate, complete, and consistent. However, computers are unable to provide or protect all of these qualities. Therefore, in the computer security field, integrity is often discussed more narrowly as having two

Location of Selected Security Topics

Because this handbook is structured to focus on computer security controls, there may be several security topics that the reader may have trouble locating. For example, no separate section is devoted to mainframe or personal computer security, since the controls discussed in the handbook can be applied (albeit in different ways) to various processing platforms and systems. The following may help the reader locate areas of interest not readily found in the table of contents:

Topic	**Chapter**	
Accreditation	8. 9.	Life Cycle Assurance
Firewalls	17.	Logical Access Controls
Security Plans	8.	Life Cycle
Trusted Systems	9.	Assurance
	Security features, including those incorporated into trusted systems, are discussed throughout.	
Viruses & Other Malicious Code	9. 12.	Assurance (Operational Assurance section) Incident Handling
Network Security	Network security uses the same basic set of controls as mainframe security or PC security. In many of the handbook chapters, considerations for using the control is a networked environment are addressed, as appropriate. For example, secure gateways are discussed as a part of Access Control; transmitting authentication data over insecure networks is discussed in the Identification and Authentication chapter; and the Contingency Planning chapter talks about data communications contracts. For the same reason, there is not a separate chapter for PC, LAN, minicomputer, or mainframe security.	

facets: *data integrity* and *system integrity.* "Data integrity is a requirement that information and programs are changed only in a specified and authorized manner."[6] System integrity is a requirement that a system "performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system."[7] The definition of *integrity* has been, and continues to be, the subject of much debate among computer security experts.

---

[6] National Research Council, *Computers at Risk*, (Washington, DC: National Academy Press, 1991), p. 54.

[7] National Computer Security Center, Pub. NCSC-TG-004-88.

Availability: A "requirement intended to assure that systems work promptly and service is not denied to authorized users."[8]

Confidentiality: A requirement that private or confidential information not be disclosed to unauthorized individuals.

1.5 Legal Foundation for Federal Computer Security Programs

The executive principles discussed in the next chapter explain the need for computer security. In addition, within the federal government, a number of laws and regulations mandate that agencies protect their computers, the information they process, and related technology resources (e.g., telecommunications).[9] The most important are listed below.

- The *Computer Security Act of 1987* requires agencies to identify sensitive systems, conduct computer security training, and develop computer security plans.
- The *Federal Information Resources Management Regulation* (FIRMR) is the primary regulation for the use, management, and acquisition of computer resources in the federal government.
- *OMB Circular A-130* (specifically Appendix III) requires that federal agencies establish security programs containing specified elements.

Note that many more specific requirements, many of which are agency specific, also exist.

Federal managers are responsible for familiarity and compliance with applicable legal requirements. However, laws and regulations do not normally provide detailed instructions for protecting computer-related assets. Instead, they specify requirements – such as restricting the availability of personal data to authorized users. This handbook aids the reader in developing an effective, overall security approach and in selecting cost-effective controls to meet such requirements.

References

Auerbach Publishers (a division of Warren Gorham & Lamont). *Data Security Management*. Boston, MA. 1995.

British Standards Institute. *A Code of Practice for Information Security Management*, 1993.

Caelli, William, Dennis Longley, and Michael Shain. *Information Security Handbook*. New

---

[8] *Computers at Risk*, p. 54.

[9] Although not listed, readers should be aware that laws also exist that may affect nongovernment organizations.

York, NY: Stockton Press, 1991.

Fites, P., and M. Kratz. *Information Systems Security: A Practitioner's Reference.* New York, NY: Van Nostrand Reinhold, 1993.

Garfinkel, S., and G. Spafford. *Practical UNIX Security.* Sebastopol, CA: O'Riley & Associates, Inc., 1991.

Institute of Internal Auditors Research Foundation. *System Auditability and Control Report.* Altamonte Springs, FL: The Institute of Internal Auditors, 1991.

National Research Council. *Computers at Risk: Safe Computing in the Information Age.* Washington, DC: National Academy Press, 1991.

Pfleeger, Charles P. *Security in Computing.* Englewood Cliffs, NJ: Prentice Hall, 1989.

Russell, Deborah, and G.T. Gangemi, Sr. *Computer Security Basics.* Sebastopol, CA: O'Reilly & Associates, Inc., 1991.

Ruthberg, Z., and Tipton, H., eds. *Handbook of Information Security Management.* Boston, MA: Auerbach Press, 1993.

Chapter 2

ELEMENTS OF COMPUTER SECURITY

This handbook's general approach to computer security is based on eight major elements:

1. Computer security should support the mission of the organization.
2. Computer security is an integral element of sound management.
3. Computer security should be cost-effective.
4. Computer security responsibilities and accountability should be made explicit.
5. System owners have computer security responsibilities outside their own organizations.
6. Computer security requires a comprehensive and integrated approach.
7. Computer security should be periodically reassessed.
8. Computer security is constrained by societal factors.

Familiarity with these elements will aid the reader in better understanding how the security controls (discussed in later sections) support the overall computer security program goals.

2.1 Computer Security Supports the Mission of the Organization.

The purpose of computer security is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. Unfortunately, security is sometimes viewed as thwarting the mission of the organization by imposing poorly selected, bothersome rules and procedures on users, managers, and systems. On the contrary, well-chosen security rules and procedures do not exist for their own sake – they are put in place to protect important assets and thereby support the overall organizational mission.

Security, therefore, is a means to an end and not an end in itself. For example, in a private-sector business, having good security is usually secondary to the need to make a profit. Security, then, *ought to* increase the firm's ability to make a profit. In a public-sector agency, security is usually secondary to the agency's service provided to citizens. Security, then, *ought to* help improve the service provided to the citizen.

To act on this, managers need to understand both their organizational mission and how each information system supports that mission. After a system's role has been defined, the security requirements implicit in that role can be defined. Security can then be explicitly stated in terms of the organization's mission.

The roles and functions of a system may not be constrained to a single organization. In an interorganizational system, each organization benefits from securing the system. For example, for electronic commerce to be successful, each of the participants requires security controls to protect their resources. However, good security on the buyer's system also benefits the seller; the buyer's system is less likely to be used for fraud or to be unavailable or otherwise negatively affect the seller. (The reverse is also true.)

2.2 Computer Security is an Integral Element of Sound Management.

Information and computer systems are often critical assets that support the mission of an organization. Protecting them can be as critical as protecting other organizational resources, such as money, physical assets, or employees.

However, including security considerations in the management of information and computers does not completely eliminate the possibility that these assets will be harmed. Ultimately, organization managers have to decide what the level of risk they are willing to accept, taking into account the cost of security controls.

This chapter draws upon the OECD's *Guidelines for the Security of Information Systems*, which was endorsed by the United States. It provides for:

Accountability - The responsibilities and accountability of owners, providers and users of information systems and other parties...should be explicit.

Awareness - Owners, providers, users and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures...for the security of information systems.

Ethics - The Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interest of others are respected.

Multidisciplinary - Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints....

Proportionality - Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm....

Integration - Measures, practices and procedures for the security of information systems should be coordinated and integrated with each other and other measures, practices and procedures of the organization so as to create a coherent system of security.

Timeliness - Public and private parties, at both national and international levels, should act in a timely coordinated manner to prevent and to respond to breaches of security of information systems.

Reassessment - The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

Democracy - The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.

As with many other resources, the management of information and computers may transcend organizational boundaries. When an organization's information and computer systems are linked with external systems, management's responsibilities also extend beyond the organization. This may require that management (1) know what general level or type of security is employed on the external system(s) or (2) seek assurance that the external system provides adequate security for the using organization's needs.

2.3 Computer Security Should Be Cost-Effective.

The costs and benefits of security should be carefully examined *in both monetary and non-monetary terms* to ensure that the cost of controls does not exceed expected benefits. Security should be appropriate and proportionate to the value of and degree of reliance on the computer systems and to the severity, probability and extent of potential harm. Requirements for security vary, depending upon the particular computer system.

In general, security is a smart business practice. By investing in security measures, an organization can reduce the frequency and severity of computer security-related losses. For example, an organization may estimate that it is experiencing significant losses per year in inventory through fraudulent manipulation of its computer system. Security measures, such as an improved access control system, may significantly reduce the loss.

Moreover, a sound security program can thwart hackers and can reduce the frequency of viruses. Elimination of these kinds of threats can reduce unfavorable publicity as well as increase morale and productivity.

Security benefits, however, do have both direct and indirect costs. Direct costs include purchasing, installing, and administering security measures, such as access control software or fire-suppression systems. Additionally, security measures can sometimes affect system performance, employee morale, or retraining requirements. All of these have to be considered in addition to the basic cost of the control itself. In many cases, these additional costs may well exceed the initial cost of the control (as is often seen, for example, in the costs of administering an access control package). Solutions to security problems should not be chosen if they cost more, directly or indirectly, than simply tolerating the problem.

2.4 Computer Security Responsibilities and Accountability Should Be Made Explicit.

The responsibilities and accountability[10] of owners, providers, and users of computer systems and other parties[11] concerned with the security of computer systems should be explicit.[12] The assignment of responsibilities may be internal to an organization or may extend across organizational boundaries.

Depending on the size of the organization, the program may be large or small, even a collateral duty of another management official. However, even small organizations can prepare a document that states organization policy and makes explicit computer security responsibilities. This element does *not* specify that individual accountability must be provided for on all systems. For example, many information dissemination systems do not require user identification and, therefore, cannot hold users accountable.

2.5 Systems Owners Have Security Responsibilities Outside Their Own Organizations.

If a system has external users, its owners have a responsibility to share appropriate knowledge about the existence and general extent of security measures so that other users can be *confident* that the system is adequately secure. (This does not imply that all systems must meet any minimum level of security, but does imply that system owners should inform their clients or users about the nature of the security.)

In addition to sharing information about security, organization managers "should act in a timely, coordinated manner to prevent and to respond to breaches of security" to help prevent damage to

---

[10] The difference between responsibility and accountability is not always clear. In general, ***responsibility*** is a broader term, defining obligations and expected behavior. The term implies a proactive stance on the part of the responsible party and a causal relationship between the responsible party and a given outcome. The term *accountability* generally refers to the ability to hold people responsible for their actions. Therefore, people could be responsible for their actions but not held accountable. For example, an anonymous user on a system is responsible for not compromising security but cannot be held accountable if a compromise occurs since the action cannot be traced to an individual.

[11] The term *other parties* may include but is not limited to: executive management; programmers; maintenance providers; information system managers (software managers, operations managers, and network managers); software development managers; managers charged with security of information systems; and internal and external information system auditors.

[12] Implicit is the recognition that people or other entities (such as corporations or governments) *have* responsibilities and accountability related to computer systems. These are responsibilities and accountabilities are often shared among many entities. (Assignment of responsibilities is usually accomplished through the issuance of policy. See Chapter 5.)

others.[13] However, taking such action should *not* jeopardize the security of systems.

2.6 Computer Security Requires a Comprehensive and Integrated Approach.

Providing effective computer security requires a comprehensive approach that considers a variety of areas both within and outside of the computer security field. This comprehensive approach extends throughout the entire information life cycle.

2.6.1 Interdependencies of Security Controls

To work effectively, security controls often depend upon the proper functioning of other controls. In fact, many such interdependencies exist. If appropriately chosen, managerial, operational, and technical controls can work together synergistically. On the other hand, without a firm understanding of the interdependencies of security controls, they can actually undermine one another. For example, without proper training on how and when to use a virus-detection package, the user may apply the package incorrectly and, therefore, ineffectively. As a result, the user may mistakenly believe that their system will always be virus-free and may inadvertently spread a virus. In reality, these interdependencies are usually more complicated and difficult to ascertain.

2.6.2 Other Interdependencies

The effectiveness of security controls also depends on such factors as system management, legal issues, quality assurance, and internal and management controls. Computer security needs to work with traditional security disciplines including physical and personnel security. Many other important interdependencies exist that are often unique to the organization or system environment. Managers should recognize how computer security relates to other areas of systems and organizational management.

2.7 Computer Security Should Be Periodically Reassessed.

Computers and the environments they operate in are dynamic. System technology and users, data and information in the systems, risks associated with the system and, therefore, security requirements are ever-changing. Many types of changes affect system security: technological developments (whether adopted by the system owner or available for use by others); connecting to external networks; a change in the value or use of information; or the emergence of a new threat.

---

[13] Organisation for Economic Co-operation and Development, *Guidelines for the Security of Information Systems*, Paris, 1992.

In addition, security is *never* perfect when a system is implemented. System users and operators discover new ways to intentionally or unintentionally bypass or subvert security. Changes in the system or the environment can create new vulnerabilities. Strict adherence to procedures is rare, and procedures become outdated over time. All of these issues make it necessary to reassess the security of computer systems.

2.8 Computer Security is Constrained by Societal Factors.

The ability of security to support the mission of the organization(s) may be limited by various factors, such as social issues. For example, security and workplace privacy can conflict. Commonly, security is implemented on a computer system by identifying users and tracking their actions. However, expectations of privacy vary and can be violated by some security measures. (In some cases, privacy may be mandated by law.)

Although privacy is an extremely important societal issue, it is not the only one. The flow of information, especially between a government and its citizens, is another situation where security may need to be modified to support a societal goal. In addition, some authentication measures, such as retinal scanning, may be considered invasive in some environments and cultures.

The underlying idea is that security measures should be selected and implemented with a recognition of the rights and legitimate interests of others. This many involve balancing the security needs of information owners and users with societal goals. However, rules and expectations change with regard to the appropriate use of security controls. These changes may either increase or decrease security.

The relationship between security and societal norms is not necessarily antagonistic. Security can enhance the access and flow of data and information by providing more accurate and reliable information and greater availability of systems. Security can also increase the privacy afforded to an individual or help achieve other goals set by society.

References

Organisation for Economic Co-operation and Development. *Guidelines for the Security of Information Systems.* Paris, 1992.

Chapter 3

ROLES AND RESPONSIBILITIES

One fundamental issue that arises in discussions of computer security is: "Whose responsibility is it?" Of course, on a basic level the answer is simple: computer security is the responsibility of everyone who can affect the security of a computer system. However, the specific duties and responsibilities of various individuals and organizational entities vary considerably.

This chapter presents a brief overview of roles and responsibilities of the various officials and organizational offices *typically* involved with computer security.[14] They include the following groups:[15]

- senior management
- program/functional managers/application owners,
- computer security management,
- technology providers,
- supporting organizations, and
- users.

This chapter is intended to give the reader a basic familiarity with the major organizational elements that play a role in computer security. *It does not describe all responsibilities of each in detail, nor will this chapter apply uniformly to all organizations.* Organizations, like individuals, have unique characteristics, and no single template can apply to all. Smaller organizations, in particular, are not likely to have separate individuals performing many of the functions described in this chapter. Even at some larger organizations, some of the duties described in this chapter may not be staffed with full-time personnel. What is important is that these *functions* be handled in a manner appropriate for the organization.

As with the rest of the handbook, *this chapter is not intended to be used as an audit guide*.

---

[14] Note that this includes groups *within* the organization; outside organizations (e.g., NIST and OMB) are not included in this chapter.

[15] These categories are generalizations used to help aid the reader; if they are not applicable to the reader's particular environment, they can be safely ignored. While all these categories may not exist in a particular organization, the functionality implied by them will often still be present. Also, some organizations may fall into more than one category. For example, the personnel office both supports the computer security program (e.g., by keeping track of employee departures) and is also a user of computer services.

3.1 Senior Management

Senior management has ultimate responsibility for the security of an organization's computer systems.

Ultimately, responsibility for the success of an organization lies with its senior managers. They establish the organization's computer security program and its overall program goals, objectives, and priorities in order to support the mission of the organization. Ultimately, the head of the organization is responsible for ensuring that adequate resources are applied to the program and that it is successful. Senior managers are also responsible for setting a good example for their employees by following all applicable security practices.

3.2 Computer Security Management

The *Computer Security Program Manager* (and support staff) directs the organization's day-to-day management of its computer security program. This individual is also responsible for coordinating all security-related interactions among organizational elements involved in the computer security program – as well as those external to the organization.

3.3 Program and Functional Managers/Application Owners

Program or Functional Managers/Application Owners are responsible for a program or function (e.g., procurement or payroll) including the supporting computer system.[16] Their responsibilities include providing for appropriate security, including management, operational, and technical controls. These officials are usually assisted by a technical staff that oversees the actual workings of the system. This kind of support is no different for other staff members who work on other program implementation issues.

Also, the program or functional manager/application owner is often aided by a *Security Officer* (frequently dedicated to that system, particularly if it is large or critical to the organization) in developing and implementing security requirements.

3.4 Technology Providers

System Management/System Administrators. These personnel are the managers and technicians who design and operate computer systems. They are responsible for implementing technical security on computer systems and for being familiar with security technology that relates to their system. They also need to ensure the continuity of their services to meet the needs of functional managers as well as analyzing technical vulnerabilities in their systems (and their security

---

[16] The functional manager/application owner may or may not be the *data owner*. Particularly within the government, the concept of the data owner may not be the most appropriate, since citizens ultimately own the data.

implications). They are often a part of a larger Information Resources Management (IRM) organization.

Communications/Telecommunications Staff. This office is normally responsible for providing communications services, including voice, data, video, and fax service. Their responsibilities for communication systems are similar to those that systems management officials have for their systems. The staff may not be separate from other technology service providers or the IRM office.

System Security Manager/Officers. Often assisting system management officials in this effort is a *system security manager/officer* responsible for day-to-day security implementation/administration duties. Although not normally part of the computer security program management office, this officer is responsible for coordinating the security efforts of a particular system(s). This person works closely with system management personnel, the computer security program manager, and the program or functional manager's security officer. In fact, depending upon the organization, this may be the same individual as the program or functional manager's security officer. This person may or may not be a part of the organization's overall security office.

Help Desk. Whether or not a Help Desk is tasked with incident handling, it needs to be able to recognize security incidents and refer the caller to the appropriate person or organization for a response.

What is a Program/Functional Manager?

The term *program/functional manager* or *application owner* may not be familiar or immediately apparent to all readers. The examples provided below should help the reader better understand this important concept. In reviewing these examples, note that computer systems often serve more than one group or function.

Example 1. A personnel system serves an entire organization. However, the Personnel Manager would normally be the application owner. This applies even if the application is distributed so that supervisors and clerks throughout the organization use and update the system.

Example #2. A federal benefits system provides monthly benefit checks to 500,000 citizens. The processing is done on a mainframe data center. The Benefits Program Manager is the application owner.

Example 3. A mainframe data processing organization supports several large applications. The mainframe director is *not* the Functional Manager for any of the applications.

Example 4. A 100-person division has a diverse collection of personal computers, work stations, and minicomputers used for general office support, Internet connectivity, and computer-oriented research. The division director would normally be the Functional Manager responsible for the system.

3.5 Supporting Functions[17]

The security responsibilities of managers, technology providers and security officers are supported by functions normally assigned to others. Some of the more important of these are described below.

Audit. Auditors are responsible for examining systems to see whether the system is meeting stated security requirements, including system and organization policies, and whether security controls are appropriate. Informal audits can be performed by those operating the system under review or, if impartiality is important, by outside auditors.[18]

Physical Security. The physical security office is usually responsible for developing and enforcing appropriate physical security controls, in consultation with computer security management, program and functional managers, and others, as appropriate. Physical security should address not only central computer installations, but also backup facilities and office environments. In the government, this office is often responsible for the processing of personnel background checks and security clearances.

Who Should Be the Accrediting Official?

The Accrediting Officials are agency officials who have authority to accept an application's security safeguards and approve a system for operation. The Accrediting Officials must also be authorized to allocate resources to achieve acceptable security and to remedy security deficiencies. Without this authority, they cannot realistically take responsibility for the accreditation decision. In general, Accreditors are senior officials, who may be the Program or Function Manager/Application Owner. For some very sensitive applications, the Senior Executive Officer is appropriate as an Accrediting Official. In general, the more sensitive the application, the higher the Accrediting Officials are in the organization.

Where privacy is a concern, federal managers can be held personally liable for security inadequacies. The issuing of the accreditation statement fixes security responsibility, thus making explicit a responsibility that might otherwise be implicit. Accreditors should consult the agency general counsel to determine their personal security liabilities.

Note that accreditation is a formality unique to the government.

Source: NIST FIPS 102

Disaster Recovery/Contingency Planning Staff. Some organizations have a separate disaster recovery/contingency planning staff. In this case, they are normally responsible for contingency planning for the organization as a whole, and normally work with program and functional mangers/application owners, the computer security staff, and others to obtain additional contingency planning support, as needed.

---

[17] Categorization of functions and organizations in this section as supporting is in no way meant to imply any degree of lessened importance. Also, note that this list is not all-inclusive. Additional supporting functions that can be provided may include configuration management, independent verification and validation, and independent penetration testing teams.

[18] The term *outside auditors* includes both auditors external to the organization as a whole and the organization's internal audit staff. For purposes of this discussion, both are outside the management chain responsible for the operation of the system.

Quality Assurance. Many organizations have established a quality assurance program to improve the products and services they provide to their customers. The quality officer should have a working knowledge of computer security and how it can be used to improve the quality of the program, for example, by improving the integrity of computer-based information, the availability of services, and the confidentiality of customer information, as appropriate.

Procurement. The procurement office is responsible for ensuring that organizational procurements have been reviewed by appropriate officials. The procurement office cannot be responsible for ensuring that goods and services meet computer security expectations, because it lacks the technical expertise. Nevertheless, this office should be knowledgeable about computer security standards and should bring them to the attention of those requesting such technology.

Training Office. An organization has to decide whether the primary responsibility for training users, operators, and managers in computer security rests with the training office or the computer security program office. In either case, the two organizations should work together to develop an effective training program.

Personnel. The personnel office is normally the first point of contact in helping managers determine if a security background investigation is necessary for a particular position. The personnel and security offices normally work closely on issues involving background investigations. The personnel office may also be responsible for providing security-related exit procedures when employees leave an organization.

Risk Management/Planning Staff. Some organizations have a full-time staff devoted to studying all types of risks to which the organization may be exposed. This function should include computer security-related risks, although this office normally focuses on "macro" issues. Specific risk analyses for specific computer systems is normally not performed by this office.

Physical Plant. This office is responsible for ensuring the provision of such services as electrical power and environmental controls, necessary for the safe and secure operation of an organization's systems. Often they are augmented by separate medical, fire, hazardous waste, or life safety personnel.

3.6 Users

Users also have responsibilities for computer security. Two kinds of users, and their associated responsibilities, are described below.

Users of Information. Individuals who use information provided by the computer can be considered the "consumers" of the applications. Sometimes they directly interact with the system (e.g., to generate a report on screen) – in which case they are also users of the system (as discussed below). Other times, they may only read computer-prepared reports or only be briefed on such material. Some users of information may be very far removed from the computer system. Users of information are responsible for letting the functional mangers/application owners (or their representatives) know what their needs are for the protection of information, especially for its integrity and availability.

Users of Systems. Individuals who directly use computer systems (typically via a keyboard) are responsible for following security procedures, for reporting security problems, and for attending required computer security and functional training.

References

Wood, Charles Cresson. "How to Achieve a Clear Definition of Responsibilities for Information Security." DATAPRO Information Security Service, IS115-200-101, 7 pp. April 1993.