Part III
Operational Controls

Overview of Part III

This section addresses security controls that focus on controls that are, broadly speaking, implemented and executed by people. 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 can be highly interdependent with management activities as well as technical controls. The chapters, in no particular order, are:

- Personnel/User Issues
- Awareness, Training and Education
- Contingency Planning
- Computer Security Incident Handling
- Computer Support and Operations
- Physical and Environmental Protection

This section begins by addressing personnel issues. People are often cited as essential to the success of computer security -- and also, not surprisingly, as the greatest threat to security. This chapter discusses a broad range of security issues involving people, with specific emphasis on the process of granting users access to system resources. Special considerations that may arise when contractors or the public have access to the system are also presented. Two important concepts, *separation of duties* and *least privilege*, are discussed in this chapter. They show up many times throughout the Handbook, particularly in the Identification and Authentication, Logical Access Control, and Audit Trails chapters.

Closely related to the personnel chapter is the next chapter, Computer Security Awareness, Training, and Education. This chapter defines and discusses benefits and differences among awareness, training, and education. General implementation issues are also presented.

Next, the Handbook focuses on contingency planning and incident handling, two chapters which are closely related. Both help an organization maintain the availability (and integrity and confidentiality, as necessary) of their computer resources. Contingency Planning deals with those actions that can be taken to prevent and minimize damage from harmful events as well as recover from them. The various steps involved in developing a contingency plan, as well as testing its effectiveness are discussed. The Incident Handling chapter deals specifically with deliberate malicious technical threats (e.g., hackers and viruses). This chapter presents the goals of an incident handling capability both containing and repairing damage from incidents as well as preventing future damage. Characteristics of successful incident handling programs are also reviewed.

The Computer Support and Operations chapter discusses how security is integrated into the procedures and functions taken in running a system. The chapter discusses some of the many tasks within support and operations that have significant security considerations. These include: user support, software support, configuration management, backups, media controls, documentation, and maintenance.

Physical and environmental security controls are presented in the final chapter of this section. The benefits of physical security measures are discussed, followed by specific areas of consideration, including physical access controls, fire safety, supporting utilities, structural collapse, plumbing leaks, interception of data, and mobile and portable systems. The use of physical access controls to complement logical access controls is stressed in this chapter.

10 Personnel/User Issues

10.1 Introduction

Successfully securing computers ultimately comes down to security issues involving their human users, designers, implementors, and managers. A broad range of security issues is involved in how these individuals interact with computers and the access and authorities each must have to do their job. No computer system can be said to be secure without addressing these personnel and user security issues[42].

This chapter will examine issues involved in the staffing of positions which interact with computer systems; the administration of users on a system, including considerations for terminating employee access; and special considerations which may arise when contractors or the public have access to systems.

10.2 Staffing

The staffing process generally involves at least four steps and can apply equally to general users as well as application managers, system management personnel and security personnel. These four steps include: 1) defining the job, normally involving the development of a position description; 2) determining the sensitivity of the position; 3) filling the position, which involves screening applicants (often including background checks) and selecting the individual; and 4) training the individual.

10.2.1 Groundbreaking -- Position Definition

As the managerial process of defining a position occurs, security issues should be identified and dealt with -- hopefully early in the process. Once a position has been broadly defined, the responsible supervisor must determine the type of computer access needed for the position. There are two general principles which are used by management when determining access: *separation of duties* and *least privilege*.

Separation of duties refers to the division of roles and responsibilities so that a single individual cannot subvert a critical process. For example, in accounting systems, no single individual is given authority to issue checks. Rather, one person initiates a request for a payment and another authorizes that same payment. In effect, checks and balances must be designed into both the process as well as the specific, individual positions of personnel who will implement the process. Assuring that such duties are well defined is the responsibility of the cognizant management officials.

---

[42] A distinction is made between users and personnel since some users (e.g., contractors and members of the public) may not be considered personnel (i.e., employees).

Least privilege refers to the security objective of granting users *only those accesses required to perform their duties*. Data entry clerks, for example, may not have any need to run analysis reports of their database. Least privilege may still mean that some employees have significant access, if it is required for their position. However, application of this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources.

It is critical that a supervisor carefully determine the duties, responsibilities and access levels in accordance with the principles of separation of duties and least privilege prior to actually staffing a position. Knowledge of the duties and access levels that a particular position will require is necessary for determining the sensitivity of the position.

10.2.2 Determining Position Sensitivity

During this administrative phase, another security issue must be addressed: the sensitivity of the position. The responsible management official must correctly identify those position sensitivity levels so that appropriate, cost-effective screening can be completed. This position sensitivity designation directly affects resources since screening can be costly.

> The Federal Personnel Manual provides instructions to federal managers on sensitivity classification of positions within the federal government.

Various levels of sensitivity are assigned to positions in the federal government. Determining the appropriate sensitivity level is based upon such factors as the type and level of harm (e.g., disclosure of private information, interruption of agency critical processing, computer fraud, and so forth) the individual can cause through use of the computer system as well as more traditional factors such as access to classified information and fiduciary responsibilities. The Office of Personnel Management's Federal Personnel Manual (Section 732-5, subchapter 7) provides detailed guidance on computer/ADP risk levels.[43] Three separate levels are defined, as shown below.

10.2.3 Filling the Position - Screening and Selection

Once a position's sensitivity has been determined, the position is ready to be staffed. In the federal government, this typically includes publication of a formal vacancy announcement. This is followed by a review of candidates to determine which meet the requirements of the position. More sensitive positions typically require *pre-employment* background screening while *post-employment* screening is often acceptable for less sensitive positions.

[43] There are also risk levels for other factors, such as access to national security information.

Computer/ADP Risk Levels		Adverse Impact on Computer/ADP Security
3	High Risk	Potential for exceptionally serious impact involving duties especially critical to the agency mission with broad scope and authority, and with major program responsibilities which affect a major Computer/ADP system(s)
2	Moderate Risk	Potential for moderate to serious impact involving duties of considerable importance to the agency mission with significant program responsibilities which affect large portions of a Computer/ADP system(s).
1	Low Risk	Potential for impact involving duties of limited relation to the agency mission through use of Computer/ADP system(s).

Background screening is accomplished to determine whether a particular individual is suitable to occupy a given position. For example, in positions requiring a high degree of trust, the screening process will attempt to ascertain the person's trustworthiness and the appropriateness of holding a particular position. In the federal government, the screening process is formalized through a series of background checks conducted through a central investigative office within the organization or through another organization (e.g., the Office of Personnel Management). It is again necessary to stress the importance of selecting the appropriate position sensitivity, since screening in excess of the sensitivity of the position wastes resources, while too little may cause unacceptable risks.[44]

Within the federal government, the most basic screening technique involves a check for a criminal history, checking the FBI fingerprint records, and other federal indices. More extensive background checks examine other factors such as a person's work and educational history, personal interview, possession or use of illegal substances, and interviews with current and former colleagues, neighbors, and friends. The exact type of screening that takes place depends upon the sensitivity of the position to be occupied and applicable agency implementing regulations. Screening is not conducted by the prospective employee's manager; rather, agency security and personnel officers should be consulted for agency-specific guidance.

Outside of the federal government, employee screening is accomplished in many ways. Policies vary considerably among organizations due to the sensitivity of examining an individual's background and qualifications. Organizational policies and procedures normally try to balance fears of invasiveness and slander against the need to develop confidence in the

[44] In the federal government, separate and unique screening procedures are not established for each position. Rather, positions are categorized by general sensitivity and assigned a corresponding level of background investigation or other checks.

integrity of employees. One technique may be to place the individual in a less sensitive position initially.

For both the federal government and private sector, finding something in a person's background does not necessarily mean that they are unsuitable for a particular job. A determination must be made based on the type of job, the type of finding or incident, and other relevant factors. In the federal government, this process is referred to as *adjudication*.

10.2.4 Employee Training and Awareness

Even after a candidate has been hired, the staffing process cannot yet be considered complete -- the employee must still be trained to do their job, including their computer security responsibilities and duties. As is discussed in the chapter on Training and Awareness, such security training can be very cost-effective in promoting security.

Some computer security experts argue that employees must receive initial computer security training before granting them any access to computer systems. Others argue that this must be a risk-based decision, perhaps only granting restricted access (or, perhaps, only access to their PC) until the required training is completed. Both approaches, however, recognize that adequately trained employees are crucial to the effective functioning of computer systems and applications. In addition, although training of new users is critical, it is important to recognize that security training and awareness activities should be on-going throughout the time that an individual is a system user. (See the Training and Awareness Chapter for a more thorough discussion.)

10.3 User Administration

This section describes the process of administering users and user accounts on systems. Effective administration of users' computer access is essential to maintaining system security. *User account management* focuses on both management of identification and authentication as well as access privileges. This is augmented by the process of *auditing* or otherwise periodically verifying the legitimacy of current accounts and access privileges. Finally, there are considerations involved in the *timely modification or removal of access* and associated issues for employees who are being reassigned, promoted, or terminated, or are retiring.

10.3.1 User Account Management

User account management encompasses the process of requesting, establishing, issuing, and closing user accounts. It also includes tracking of users and their respective access privileges and the management of these functions.

User account management typically begins with a request from the user's supervisor to the system manager for a system account. If a user is to have access to a particular application, this request may be sent through the application manager to the system manager. This will

assure that the systems office receives formal approval from the "application manager" for the employee to be given access. The request will normally state the level of access to be granted, perhaps by function or by specifying a particular user profile. (Often when more than one employee is doing the same job, a "profile" of permitted authorizations is created.)

Systems operations staff will normally then use the account request to create an account for the new user. The access levels of the account will be consistent with those requested by the supervisor. This account will normally be assigned selected access privileges. These are sometimes built directly into applications, and other times rely upon the operating system. "Add-on" access applications are also used. These access levels and privileges are often tied to specific access levels within an application.

Example of Access Levels within an Application

Level	Function
1	Create Records
2	Edit *Group A* records
3	Edit *Group B* records
4	Edit *all* records

Next, employees will be given their account information, including the account identifier (e.g., USERID) and means of authentication (e.g., password or smart card/PIN). One issue which frequently arises at this stage is whether the USERID is to be tied to the particular *position* an employee holds (e.g., ACC5 for an accountant) or the *individual employee* (e.g., BSMITH for Brenda Smith). This may simplify administrative overhead in some cases; however, it may make auditing more difficult as one tries to trace actions of a particular individual. However, if the USERID is created and tied to a position, procedures will have to be established to change them if employees switch jobs or are otherwise reassigned.

At the time employees are given their account it is often convenient to provide initial or refresher training and awareness on computer security issues. Users should be asked to review a set of rules and regulations for system access. To indicate their understanding of these rules, many organizations require employees to sign a "computer account receipt," which may also state causes for dismissal or prosecution under the Computer Fraud and Abuse Act and other applicable state and local laws.

When user accounts are no longer required, the supervisor should inform the application manager and IRM office so that accounts can be removed in a timely manner. One useful secondary check is to work with the local organization's personnel officer to establish a procedure for routine notification of employee departures to the systems office. Further issues are discussed in the "Termination" section below.

It is essential to realize that *access and privilege administration is a continuing process*. New users are added while old users are deleted. Permissions change: sometimes permanently, sometimes temporarily. New applications are added, upgraded and removed. Tracking this information to keep it up to date is not easy, but is necessary in order to only allow users access to those functions necessary to accomplish their assigned responsibilities -- thereby

helping to maintain the principle of *least privilege*. In managing these accounts, there is a need to balance timeliness of service and record keeping. While sound record keeping practices are necessary, delays in processing requests (e.g., change requests) may lead to requests for more access than is really necessary - just to avoid delays should such access ever be required.

Managing this process of user access is also one that, particularly for larger systems, is often decentralized. Regional offices may be will be granted the authority to create accounts and change user privileges or submit forms requesting that the centralized access control function make the necessary changes. Approval of these changes is important -- it may require the approval of the file owner and the supervisor of the employee whose access is being changed.

One example of a simple user account and password acknowledgement form is as follows:

I hereby acknowledge personal receipt of the system password(s) associated with the user IDs listed below. I understand that I am responsible for protecting the password(s), will comply with all applicable systems security standards, and will not divulge my password(s) to any person. I further understand that I must report to the Information Systems Security Officer (ISSO) any problem I encounter in the use of the password(s) or when I have reason to believe that the private nature of my password(s) has been compromised.

Detailed system security procedures, training, and guides can also be given to the employee at the time initial access is acknowledged.

10.3.2 Audit and Management Reviews

From time to time, it is necessary to review an entire system. Within the area of personnel and user issues, such reviews may examine the levels of access each individual has, consistent with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth.

These reviews can be conducted on *at least* two levels[45]: 1) an application by application basis or 2) a system-wide basis. Both kinds of reviews can be conducted by, among others, "in-house" personnel, contractor personnel, or audit personnel. For example, a good practice is for application managers may wish to review all access levels of all users of the application on a monthly basis -- and sign a formal access approval list, which will provide a formal written record of the approvals. While it initially may appear that such reviews should be conducted by systems personnel, they usually are not fully effective. System personnel *can* verify that users only have those accesses which their managers have specified. However, as noted above, these may change over time. It is therefore important to involve the application manager, who is often the only individual likely to know this information.

Outside audit organizations (e.g., the Inspector General [IG] or the General Accounting Office) may also conduct audits. For example, the IG may direct a more extensive review of

[45] Note that this is not an either-or distinction.

permissions. This may involve discussing the need for particular access levels for specific individuals or the number of users with sensitive access. For example, how many employees should really have authorization to the check printing function? (Auditors will also review non-computer access by reviewing, for example, who should have physical access to the check printer or blank stock of checks.)

10.3.3 Detecting Unauthorized / Illegal Activities

Auditing is one essential tool to detect unauthorized and illegal activities. Analysis of audit trails can yield significant insight into unauthorized activities. (See the chapter on Audit.) Other mechanisms also exist. For example, fraudulent activities may require the regular physical presence of the perpetrator(s). In such cases, the fraud may be detected during the employee's absence. Mandatory vacations, for critical systems and applications personnel can help detect such activity (however, this is not a guarantee, particularly if problems are saved for the employee to handle upon their return). It is useful to avoid creating an excessive dependence upon any single individual, since the system will have to function during the vacation period. Rotation of jobs among employees can be useful too. Periodic re-screening of personnel may also provide possible indications of illegal activity (e.g., living a lifestyle in excess of known income level).

10.3.4 Temporary Assignments and In-house Transfers

One significant aspect of managing a system involves keeping user privileges up-to-date. Privileges are typically changed under two types of circumstances: 1) change in job role, either temporarily (e.g., while covering for an employee on sick leave) or permanently (e.g., after an in-house transfer) and 2) termination. (Termination considerations are discussed in 10.4.5 below.)

Users often are required to perform duties outside their normal scope during the absence of others requiring additional access privileges. Although necessary, such extra access privileges should be granted sparingly and carefully monitored, consistent with the need to maintain separation of duties for internal control purposes. Also, they should be removed in a timely manner when no longer required.

In addition to temporary changes in access privileges, permanent changes are usually necessary when employees change positions within an organization. In this case, the process of granting account privileges (detailed in the section on "User Account Management") will occur again. At this time, however, is it also important that access privileges of the prior position be promptly removed. Many instances of "privilege creep" have occurred with employees continuing to maintain their access rights for all previously held positions within an organization. This is inconsistent with the principle of least privilege and must be avoided.

10.3.5 Termination

Termination of user's system access generally can be characterized as either "friendly" or "unfriendly." Friendly termination may occur when an employee is voluntarily transferred, resigns to accept a better position, or retires. Unfriendly termination may include situations when the user is being fired for cause, "RIFed," or being involuntarily transferred. Fortunately, the former situation is more common, but security issues must be faced in both situations.

10.3.5.1 Friendly Termination

Friendly termination refers to the removal of an employee from the organization when there is no reason to believe that the termination is other than mutually acceptable. Since terminations can be expected regularly, this is usually accomplished by implementing a standard set of procedures for outgoing or transferring employees. These are part of the standard employee "out-processing," and are put in place, for example, to ensure that system accounts are removed in a timely manner. In this case, the personnel office may send a memo to the head of the computer processing office notifying them of the employee's scheduled date of departure. But other issues must be examined by the agency as well.

The continued availability of data, for example, must often be assured. In both the manual and electronic world, this may involve documenting procedures or filing schemes. For example, how are documents stored on the hard disk and how are they backed up? Are employees instructed whether or not to "clean up" their PC before leaving? If cryptography is used to protect data, how will the availability of cryptographic keys to management personnel be assured? Who will collect access tokens? Are employees asked to document how they accomplish their tasks? What procedures are in place to make sure this is accomplished?

Confidentiality of data can be an issue as well. For example, do employees know what information they are allowed to share with their immediate organizational colleagues? Does this differ from the information they may share with the public? These and other agency specific issues should be addressed throughout an agency to assure continued access to data and to provide continued appropriate protection for its confidentiality and integrity during personnel transitions. The agency's training and awareness program should address such issues, as appropriate.

10.3.5.2 Unfriendly Termination

Unfriendly termination describes the situation when the removal of the employee takes place under involuntary or adverse conditions. This may include termination for cause, RIF reduction, involuntary transfer, resignation for "personality conflicts," situations with pending grievances, and so forth. The tension in such terminations may multiply and complicate security issues which must be faced. Additionally, all of the issues involved in friendly terminations are still present, but addressing them may be considerably harder.

The greatest threat from unfriendly terminations is likely to come from those with the capability to change code or modify the system or applications. For example, systems personnel are ideally positioned to wreak considerable havoc on systems operations. Without appropriate safeguards, personnel with such access can place logic bombs (e.g., a hidden program to erase a disk) in code which will not even execute until after the employee's departure. Backup copies can be destroyed. There are even examples where code has been "held hostage." But other employees, such as general users, can also cause damage. Errors can be input purposefully. Documentation can be misfiled. Other "random" errors can be made. Correcting these situations can be resource intensive.

Given the potential for adverse consequences, security specialists routinely recommend that system access be terminated as quickly as possible in such situations. If an employee is to be fired, system access should be removed at the same time (or just before) the employee is notified of their dismissal. When an employee notifies an agency of a resignation and it can be reasonably expected that it is on unfriendly terms, system access should be immediately terminated. During the "notice" period, it may be necessary to assign the individual to a restricted area and function. This may be particularly true for those with the capability to change programs or modify the system or applications. In other cases, physical removal from their offices (and, of course, logical removal, *when logical access controls exist*) may suffice.

In addition to those with the ability to change programs or modify systems or applications, users also present a security risk which must not be overlooked during the termination process.

10.4 Contractor Access Considerations

Many federal agencies as well as private organizations utilize contractors and consultants to aid their computer processing. Within the federal government, use of non-government employees, whose organizational loyalties may lie other than with the government agency, could raise serious concerns.

Contractors are often, but not always, utilized for shorter periods of time than regular federal government employees. This factor may change the cost-effectiveness of conducting pre- and post-"employment" screening. Screening which may be standard for employees may not necessarily be consistent with the employment practices, procedures, and policies of the contractor. (In some such cases, it may be appropriate for the agency to consider finding another contractor.) The often higher turnover among contractor personnel entails additional costs for security programs in terms of user administration, particularly for privileged accounts if the contractors are managing the system.

Contractors are also widely used for systems maintenance. This raises issues such as:

- To what data and files should maintenance personnel be granted access? How will contractors be prevented from unauthorized access to proprietary software or other

contractors' proprietary data?

- Is the need for such access continuing or sporadic (and what are the associated costs of granting, removing, and auditing such changes)?

- Is contractor/maintenance access to be local or remote? If remote, are necessary security measures in place to reduce the risk of unauthorized system access or disclosure of data requiring confidentiality protection?

Answers to these questions will vary from organization to organization, but indicate the level of detailed thought that must be undertaken for contractor access.

10.5 Public Access Considerations

Many federal agencies have begun to design, develop, and implement public access systems for electronic dissemination of information to the public. Some systems provide electronic interaction by allowing the public to send information to the government (e.g., electronic tax filing) as well as receive it. When systems are made available for access by the public (or a large or significant subset thereof), additional security issues arise due to: 1) increased threats against public access systems and 2) the difficulty of security administration.

While many computer systems have been victims of hacker attacks, public access systems are well-known and have published phone numbers and network access IDs. In addition, a successful attack could result in a lot of publicity. For these reasons, public access systems are subject to a greater threat from hacker attacks. In general, it is safe to say that when a system is made available for public access, the risk to the system increases -- and often the constraints on its use are tightened.

Hackers can attack the confidentiality, availability and integrity of information processed by a system. Public access systems are often highly visible targets for hackers. Besides increased risk of hackers, public access systems can also be subject to insider malice. For example, an unscrupulous user, such as a disgruntled employee, may try to introduce errors into data files intended for distribution to embarrass or discredit the agency. Attacks on public access systems could have a substantial impact upon the agency's reputation and the level of public confidence due to the higher visibility of public access systems. Other security problems may arise from unintentional actions by untrained users.

In systems without public access, there are procedures for enrolling users which often involve some user training and frequently the signing of forms acknowledging user responsibilities. In addition, user profiles can be created and sophisticated audit mechanisms developed to detect unusual activity by a user. In public access systems, users are often anonymous. This can complicate system security administration.

In most systems without public access, users are typically a mix of known employees or

contractors. In this case, imperfectly implemented access control schemes (where they are required) may be tolerated. However, when opening up a system to public access, additional precautions may be necessary because of the increased threats. In this situation, strict attention to the implementation of access controls becomes all the more crucial.

10.6 Interdependencies

Personnel and user related issues are tied to topics throughout this Handbook. However, two of particular importance are:

> *Training and Awareness* is a critical part of addressing the personnel and user issues of computer security, which is discussed in a separate chapter.
>
> *Identification and Authentication* and *Access Controls* in a computer system can only prevent people from doing what the computer is instructed they are not allowed to do, as stipulated by *Policy*. The recognition by computer security experts that much more harm comes from people doing what they are allowed to do, but should not, points to the importance of considering personnel and user issues in the computer security picture, and the importance of *Auditing*.
>
> *Personnel* issues are closely linked to policy, and particularly its *compliance* component. A deterrent effect arises among users when they are aware of the fact that their misconduct, intentional or unintentional, will be caught.

These controls also depend on 1) managers selecting the right type and level of access for their employees and 2) informing system managers of which employees need accounts, what type and level of access they require, and informing the system managers of changes to access requirements in a timely manner. Otherwise, accounts and accesses can be granted to or maintained for people who should not have them.

10.7 Cost Considerations

There are many security costs which fall under the category of personnel and user issues. Among these are:

> *Screening*, which includes costs of initial background screening and periodic updates, as appropriate[46];
>
> *Training and Awareness* - costs of training needs assessments, training materials, course fees, and so forth, as discussed separately in the Training and Awareness;

[46] When analyzing the costs of screening, it is important to realize that screening is often accomplished to meet requirements wholly unrelated to computer security.

User Administration - costs of identification and authentication management which, particularly for large distributed systems, may be rather significant;

Access and Privilege Administration - particularly beyond the initial account set-up, are on-going costs of maintaining user accesses current and complete.

Auditing, although such costs can be reduce somewhat when using automated tools, consistent, resource-intensive human review is still often necessary to detect and resolve security anomalies.

10.8 Summary

This chapter reviewed the major security issues involved with personnel and other users. These include the staffing and screening of employees for positions and management of user privileges. Particularly important, and not to be under-stressed, are security issues involved in user administration, including identification and authentication management and access and privilege administration. The utility of audit and other management reviews in detecting unauthorized and illegal activities was also reviewed, as were security issues involved in removing access privileges for both friendly and unfriendly terminations. Finally, the chapter discussed some issues which arise when non-employees, particularly contractors and members of the public, are granted access to the system.

10.9 References

Federal Personnel Manual (especially Chapters 732 - 735). Office of Personnel Management.

North, S. "To Catch a 'Crimoid'." *Beyond Computing*. 1(1), 1992. pp. 55-56.

Pankau, E. "The Consummate Investigator." *Security Management*. 37(2), 1993. pp. 37-41.

Schou, C. W. Machonachy, F. Lynn McNulty and A. Chantker. "Information Security Professionalism for the 1990s." *Computer Security Journal*. 9(1), 1992. pp. 27-38.

"Security Issues in Public Access Systems." Computer Systems Lab Bulletin. May, 1993.

Wagner, M. "Possibilities are Endless, and Frightening." *Open Systems Today*. November 8 (136), 1993. pp. 16-17.

Wood, C. "Be Prepared Before You Fire." *Infosecurity News*. 5(2), 1994. pp. 51-54.

Wood, C. "Duress Terminations and Information Security." *Computers and Security*. 12(6), 1993. pp. 527-535.

11 Preparing for Contingencies and Disasters

11.1 Introduction

Contingency planning directly supports an organization's goal of continued operations. Organizations practice contingency planning because it makes good business sense.

The purpose of preparing for contingencies and disasters is to provide for the continuation of critical missions and business functions in the event of disruptions. A disruption could be caused by many events such as a power outage, hardware failure, fire or storm. A *computer security contingency* is an event that disrupts computer operations thereby disrupting mission and business functions. If the event is very destructive, it is often called a disaster.[47]

The preparation for handling contingencies and disasters is generally called *contingency planning* although it has many names (e.g., disaster recovery, business continuity, continuity of operations, or business resumption planning).

A second purpose of contingency planning is to minimize the effect of disruptions. Many potential contingencies and disasters can be averted or the damage they cause can be reduced if the correct steps are taken early to control the event.

Contingency planning is more than moving offsite after a disaster destroys a data center. Contingency planning addresses how an organization operates and how to keep the critical functions operating in the event of disruptions, both large and small. This broader perspective on contingency planning is based on the distribution of computer support throughout an organization.

This chapter divides the contingency planning process into six steps.[48] These steps describe basic principles of contingency planning. The six steps are:

1) *Identifying the mission or business critical functions*. This includes both the identification and prioritization of critical functions.

2) *Identifying the resources that support the critical functions.* This includes identifying what combination of resources is needed and when they are needed.

[47] There is no distinct dividing line between disasters and other contingencies.

[48] Some organizations and methodologies may use a different order, nomenclature, number, or combination of steps. The specific steps can be modified as long as the basic principles are addressed.

3) *Anticipating potential contingencies or disasters*. This develops a range of the types of contingencies that could affect the organization's critical functions and resources.

4) *Selecting contingency planning strategies*. This includes evaluating and selecting strategies to recover from contingencies. The strategy should also address the resumption of normal operations.

5) *Implementing the strategy*. This step includes the preparations that must be done to be ready for contingencies.

Six Basic Steps of Contingency Planning

1. Identifying critical functions
2. Identifying critical resources
3. Anticipating potential contingencies
4. Selecting contingency strategies
5. Implementing the strategies
6. Testing & revising

6) *Testing and revising*. This step involves testing any of the strategies or the preparation.

This chapter will briefly explain each of the six steps. In addition, the chapter will discuss some of the basic implementation considerations, including development of the organization's approach to contingency planning and coordination among the organization's components.

11.2 Step #1: Identifying the Mission or Business Critical Functions

It is quite difficult to protect the continuity of an organization's mission or business if it is not clearly identified. This step requires managers to understand the organization from a broader point of view -- wider than the area the manager controls. The definition of an organization's critical mission or business functions is often called a *business plan*.

This chapter refers to an organization as having critical *mission* or *business* functions. In government organizations, the focus is normally on performing a mission, such as providing citizen benefits. In private organizations, the focus is normally on performing a business, such as manufacturing widgets.

Since the development of a business plan will be used to support contingency planning, it is necessary to not only identify critical missions and businesses, but to *prioritize* them. A fully redundant capability for each function is prohibitively expensive for most organizations. In the event of a disaster, certain functions will not be performed. If this prioritization has not been correctly accomplished by senior management, it will delay the recovery of critical functions. This will increase the damage contingencies can cause an organization and could be the difference between surviving a disaster or not.

11.3 Step #2: Identifying the Resources that Support Critical Functions

In many cases, the longer an organization is without a resource, the more critical the situation becomes.

After identifying critical missions and business functions, it is necessary to identify the supporting resources and the timeframe in which the resource is used (e.g., is the resource needed constantly? or only at the end of the month?). In identifying resources, a traditional problem has been that different managers oversee different resources. They may not realize how the resources interact to perform the organization's mission or business.

Many of these resources are *not* computer resources. Contingency planning should address all the resources needed to perform a function, whether they relate to a computer or not.[49]

The analysis of needed resources should be done by people who really understand how the function is performed. In addition, they must understand the dependencies of various resources on other resources and other critical relationships between the resources. This will allow an organization to *prioritize* resources. Not all elements of all resources are crucial to the critical functions.

11.3.1 Human Resources

Resources that Support Critical Functions

Human Resources
Processing Capability
Computer-Based Services
Data & Applications
Physical Infrastructure
Documents & Papers

People are perhaps the most obvious resource. Some functions require the effort of specific people, some require people with specialized expertise, and some only require people who can be trained to perform a specific task. Within the information technology field, people include both operators (such as technicians or system programmers) or users (such as data entry clerks or information analysts).

11.3.2 Processing Capability

Traditional contingency planning focused on processing power, (i.e., if the mainframe was down, how could applications dependent on the mainframe continue to be processed?). The need for mainframe backup is still vital; however, other processing platforms are also important. LANs, minicomputers, workstations, and personal computers in all forms of centralized and distributed processing may be performing critical tasks.

[49] However, since this is a computer security handbook, the descriptions below focus on the computer-related resources. The logistics of coordinating contingency planning for computer-related and other resources is an important consideration.

11.3.3 Automated Applications and Data

Computer systems run applications and process data. Without current electronic versions of both the applications and the data, computerized processing may not be able to occur. If the processing is being performed on alternate hardware, it is necessary for the applications to be compatible with the alternate hardware.

11.3.4 Computer-Based Services

There are many different kinds of computer-based services used by an organization to perform its functions. The two most important are normally communications services and information services. Communications can be further categorized as data and voice; however, in many organizations these are performed by the same service. Information services include any source of information outside of the organization. Many of these sources are becoming automated, including online government and private databases, news services or bulletin boards.

Contingency Planning Teams

In order to understand what resources are needed from each of these categories and to understand how the resources support critical functions, it is often necessary to establish a contingency planning team. The team would contain representatives from various organizational elements, often headed by a contingency planning coordinator. A typical team involves representatives from the following three groups:

(1) business-oriented, such as representatives from functional areas;

(2) facilities management; and

(3) technology management.

Various other groups are called on as needed including financial management, personnel, training, safety, computer security, physical security or public affairs.

In addition working on the contingency planning team, these people will probably be tasked with various responsibilities after the plan is developed.

11.3.5 Physical Infrastructure

In order for people to work effectively, they need a safe working environment and appropriate equipment and utilities. This can include office space, heating, cooling, venting, power, water, sewage, other utilities, desks, telephones, fax machines, personal computers, terminals, courier services, file cabinets, and possibly many other items. In addition, computers also need space and utilities, such as electricity and often cooling. Electronic and paper media used to store applications and data also have physical requirements.

11.3.6 Documents / Papers

Many functions rely on vital records and various documents, papers, or forms. The record could be important based on a legal need (such as being able to produce a signed copy of a loan) or because that is the only place the information is recorded. Records can be maintained on paper, microfiche, microfilm, magnetic media or optical disk.

11.4 Step #3: Anticipating Potential Contingencies or Disasters

Although no one can think of *all* the various types of things that can go wrong, the next step is to identify a likely range of problems. The contingency scenarios should include small and large events. (Some experts argue that it is only necessary to plan for the worst. Others believe that small contingencies can result in major problems if not planned for.)

The development of scenarios will help an organization develop a plan to address the wide range of things that can go wrong. While some general classes of contingency scenarios are obvious, imagination and creativity, as well as research, can point to other possible contingencies which are less obvious. The contingency scenarios should address each of the resources described above. The following are *examples* of some of the types of questions that contingency scenarios should address:

Human Resources: Can people get to work? Are key personnel willing to cross a picket line? Are there critical skills and knowledge possessed by one person? Can people easily get to an alternative site?

Processing Capability: Are the computers harmed? What happens if some of the computers are inoperable, but not all?

Automated Applications and Data: Has data integrity been affected? Is an application sabotaged? Can an application run on a different processing platform?

Computer-based Services: Can the computers communicate? To where? Can people communicate? Are information services down? For how long?

Examples of Some Less Obvious Contingencies

A computer center in the basement of a building had a minor problem with rats. Exterminators killed the rats, but the bodies were not retrieved because they were hidden under the raised flooring and in the pipe conduits. Employees could only enter the data center with gas masks because of the decomposing rats.

The World Trade Center explosion created a lot of smoke and dust. When people re-entered the building, they turned on their computer systems to check for problems. Dust and smoke damaged many hard disks as the systems were turned on. If the systems had been cleaned *first*, there would not have been significant damage.

Infrastructure: Do people have a place to sit? Equipment to do their jobs? Can they occupy the building?

Documents/Paper: Can needed records be found? Are they readable?

11.5 Step #4: Selecting Contingency Planning Strategies

The next step is to plan what should happen in the event of contingencies to recover needed resources. In evaluating alternatives, it is necessary to consider what controls are in place to

prevent and minimize contingencies. Since no set of controls can cost-effectively prevent all types of contingencies, it is necessary to coordinate prevention and recovery efforts.

The selection of a strategy must be based on practical considerations including feasibility and cost. The different categories of resources should each be considered. Risk assessment can be used to help estimate the cost of options to decide on an optimal strategy. For example, is it more expensive to purchase and maintain a generator or to move processing to an alternate site considering the likelihood of losing electrical power for various lengths of time? Are the consequences of a loss of computer-related resources sufficiently high to warrant the cost of various recovery strategies? The risk assessment should be focused on areas where it is not clear which strategy is the best.

Planning to resume normal operations is an important part of contingency planning and should be part of the overall strategy.

Implicit in the idea of recovering from a contingency is the need to *resume* normal operations. Although it may appear obvious, it is necessary to *plan* to resume normal operations. This is especially true if the contingency plan calls for moving offsite. Resuming normal operations, however, is not limited to returning to the original site, but may include purchasing new equipment or moving to a new facility.

In developing contingency planning strategies, there are many factors to consider in addressing each of the resource areas described above. Some of the factors are discussed below. Some examples are presented in the sidebar on the next page.

11.5.1 Human Resources

In order to ensure an organization has access to workers with the right skills and knowledge, training and documentation of knowledge are needed. During a major contingency, people will be under significant stress and may panic. If the contingency is a regional disaster, their first concerns will probably be their family and property. In addition, many people will be either unwilling or unable to come to work. Additional hiring or temporary services can be used.

11.5.2 Processing Capability

The need for computer security does not go away when an organization is processing in a contingency mode. In some cases it may increase due to sharing processing facilities, concentrating resources in fewer sites, or using additional contractors and consultants. Security should be an important consideration when selecting contingency strategies.

Strategies for processing capability are normally grouped into four categories: 1) hot site; 2) cold site; 3) redundancy or 4) reciprocal agreements. These terms originated with recovery strategies for mainframe data centers but can be applied to other platforms. A hot site is a building already equipped with processing capability

and other services ready to go. A cold site is a building to house processors and can be easily adapted for use. A redundant site is equipped and configured exactly like the primary site. Some organizations use partial redundancy and plan on having reduced processing capability after a disaster. The stocking of spare personal computers or LAN servers also provides some redundancy. A reciprocal agreement allows two organizations to back each other up. (While this approach often sounds the best, contingency planning experts note that this alternative has the greatest chance of failure due to the problems keeping agreements and plans up-to-date as systems and personnel change.) Resumption planning may include contracts or the ability to place contracts to replace equipment.

11.5.3 Automated Applications and Data

The primary contingency strategy for applications and data is *regular backup* and secure *offsite storage*. Important decisions include how often the backup is performed, how often it is stored offsite, and how it is transported (to storage, to an alternate processing site, or to support the resumption of normal operations).

11.5.4 Computer-based Services

Service providers may offer contingency services. Voice communications carriers often can reroute calls (transparently to the user) to a new location. Data communications carriers can also reroute traffic. If the one service provider is down, it may be possible to use another. Hot sites usually have the capability to receive data and voice communications. In addition, resuming normal operations may require another rerouting of communications

Example #1: In the event that the system administrator for a LAN has to be out of the office for a long time (due to illness or an accident), arrangements are made for the system administrator of another LAN to perform the duties. Anticipating this, the absent administrator should have taken steps before hand to keep documentation current. This strategy is inexpensive, but service will probably be significantly reduced on both LANs which may prompt the manager of the loaned administrator to partially renege on the agreement.

Example #2: An organization depends on an online information service provided by a commercial vendor. The organization is no longer able to obtain the information manually within acceptable time limits and there are no other comparable services. In this case, the organization relies on the contingency plan of the service provider. The organization pays a premium to obtain priority service in case the service provider has to operate at reduced capacity.

Example #3: A large mainframe data center has a contract with a hot site vendor, a contract with the telecommunications carrier to reroute communications to the hot site, plans to move people, and stores up-to-date copies of data, applications and vital records off-site. The contingency plan is expensive, but management has decided that the expense is fully justified.

Example #4. An organization distributes its processing among three major sites, each of which includes small to medium processors (personal computers and minicomputers). If one site is lost, the remaining two can carry the load. Routing of data and voice communications can be performed transparently to redirect traffic. Data is backed up to the two other sites. This plan requires each site to have more processing capacity than needed and requires tight control over the architectures used and types of applications that are developed to ensure compatibility. In addition, personnel at all three sites must be cross-trained to perform all functions.

services.

11.5.5 Physical Infrastructure

Hot sites and cold sites discussed above may also offer office space in addition to processing capability support. Other types of contractual arrangements can be made for office space, security services, furniture, and more in the event of a contingency. If the contingency plan calls for moving off-site, procedures need to be developed to assure a smooth transition back to the primary operating facility or to a new facility.

11.5.6 Documents / Papers

The primary contingency strategy is usually backup onto magnetic, optical, microfiche, paper or other medium and offsite storage. Since paper documents are harder to backup than electronic ones, this is often done poorly. A supply of forms and other needed papers can be stored offsite.

11.6 Step #5: Implementing the Contingency Strategies

Once the strategies have been decided on it is necessary to make appropriate preparations, document the strategies, and train employees. Many of these tasks are ongoing.

11.6.1 Preparations

There are many preparations that may need to be made to implement the strategies for protecting critical functions and their supporting resources. Some examples of common types of preparation are given below.

The first example of a common preparation is to establish procedures for backing up files and applications. Another common preparation is the establishment of contracts and agreements, *if* the contingency strategy calls for them. Existing contracts for services may need to be renegotiated to add contingency services. Another preparation may be the purchase of equipment, especially to support a redundant capability.

It is important to keep preparations up-to-date. Computer systems change rapidly and so must backup services and redundant equipment. Contracts and agreements may need to reflect the changes also. If additional equipment is needed, it must be maintained and periodically replaced when it is no longer dependable or no longer fits the organization's architecture.

Backing up data files and applications is a critical part of virtually every contingency plan. Backups are used, for example, to restore files after a personal computer virus corrupts the files or after a hurricane destroys a data processing center.

The preparation should also include formally designating people who are responsible for various tasks in the event of a contingency. This group of people is often called the *contingency team*. The team is often composed of people who were a part of the contingency planning team.

11.6.2 Documentation

This is the preparation of the *contingency plan* itself. The plan must be written, kept up-to-date as the system and other factors change, and stored in a safe place. Unless written, it will be difficult to follow a plan during a contingency, especially if the person who developed the plan is unavailable. The plan should include a section that clearly states the sequence of tasks to be performed in the event of a contingency. This section should be written to allow someone with minimal knowledge to begin to execute the plan. It is generally helpful to store copies of the contingency plan in several locations, including any off-site locations such alternate processing sites, if applicable.

11.6.3 Training

Personnel must be trained in their contingency-related duties, new personnel must be trained as they join the organization, refresher training may be needed, and personnel will need to practice their skills.

Training is particularly important for effective employee response during emergency situations. There is no time to check a manual to determine correct procedures if there is a fire. Depending on the nature of the emergency, there may be time to protect equipment and other assets. Personnel must have practiced their skills in order to react correctly, especially when human safety is involved. Training can be accomplished through testing, discussed below.

11.7 Step #6: Testing and Revising

Maintenance of the contingency plan can be incorporated into computer system change management procedures so that upgrades to hardware and software are reflected in the plan.

A contingency plan should be tested periodically because there will be flaws in the plan and in its implementation. The plan will become dated as time passes and the resources used to support critical functions change. The responsibility for keeping the contingency plan current should be assigned. The extent and frequency of testing will vary between organizations and among systems. There are several types of testing including reviews, analysis, and simulations of a disaster.

A *review* can be a simple test to check the accuracy of contingency plan documentation, for instance by checking if the individuals listed are still in the organization and still have the responsibilities for which they were included in the contingency plan. This test can check

home and work telephone numbers, organizational codes, building and room numbers. The review can determine if files can be restored from backup tapes or if employees know emergency procedures.

> The results of a "test" often implies a grade assigned for a specific level of performance, or simply pass or fail. However, in the case of contingency planning, a test should be used to improve the plan. If organizations do not use this approach, then flaws in the plan may remain hidden and uncorrected.

An *analysis* may be performed on the entire plan or portions of it, such as emergency response procedures. It is beneficial if the analysis is performed by someone who did *not* help develop the contingency plan but has a good working knowledge of the critical function and supporting resources. The analyst then looks for flaws in the logic or process used by the plan developers.

Organizations can also arrange *disaster simulations*. These provide valuable information about flaws in the contingency plan and provide practice for a real emergency. While these tests can be expensive, they can also provide valuable information that can be used to ensure continuity of important functions.

11.8 Implementation

There are many important implementation issues for an organization. Two of the most important are 1) how many plans should be developed? and 2) who prepares each plan? Both of these questions revolve around the organization's overall strategy for contingency planning.

11.8.1 How Many Plans?

Some organizations have just one plan for the entire organization and others have a plan for every distinct computer system, application, or other resource. Other approaches recommend a plan for each business or mission function with separate plans, as needed, for critical resources.

> Since the answers to these questions are dependent upon the organization, it is advisable for organizations to develop contingency planning policy.

The answer to the question, therefore, depends upon the unique circumstances for each organization. But it is critical to coordinate between resource managers and functional managers who are responsible for the mission or business.

11.8.2 Who Prepares the Plan?

If an organization decides on a centralized approach to contingency planning, it may be best to name a *contingency planning coordinator*. The coordinator would prepare the plans in

cooperation with various functional and resource managers. Some organizations place responsibility directly with the functional and resource managers.

Strong project management may be needed to coordinate functional managers and resource managers. This can be especially important when prioritizing critical functions.

11.9 Interdependencies

Since all controls help to prevent contingencies, there is an interdependency with all of the controls in the Handbook.

Risk Management provides a tool for analyzing the security costs and benefits of various contingency planning options. In addition, a risk management effort can be used to help identify critical resources needed to support the organization and the likely threat to those resources. It is not necessary, however, to perform a risk assessment prior to contingency planning since the identification of critical resources can be performed during the contingency planning process itself.

Physical and Environmental Controls help prevent contingencies. Although many of the other controls, such as logical access controls, also prevent contingencies, the major threats that a contingency plan addresses are physical and environmental threats, such as fires, loss of power, plumbing breaks, or natural disasters.

Incident Handling can be viewed as a subset of contingency planning. It is the emergency response capability for various technical threats. Incident handling can also help an organization prevent future incidents.

Support and Operations in most organizations includes the periodic backing up of files. It also includes the prevention and recovery from more common contingencies, such as a disk failure or corrupted data file.

Policy is needed to create and document the organization's approach to contingency planning. The policy should explicitly assign responsibilities.

11.10 Cost Considerations

The cost of developing and implementing contingency planning strategies can be significant, especially if the strategy includes contracts for backup services or duplicate equipment. There are too many options to discuss cost considerations for each type.

One contingency cost that is often overlooked is the cost of testing a plan. Testing, however, provides many benefits and should be considered. Some of the less expensive methods, such as a review, may be sufficient for less critical resources.

A risk assessment can be used when it is unclear what contingency strategy would be most

cost-effective.

11.11 Summary

Contingency planning supports an organization's ability to perform its critical mission or business functions. The best contingency planning efforts will be based on the organization's critical functions rather than just planning to replace various resources in the event of their temporary or permanent unavailability. Therefore, although technology managers are a very important component of effective contingency planning, it is functional managers who should provide the impetus. Since effective contingency planning can cross many organizational boundaries among both functional managers and resources providers, clear policy guidance and strong project management may be needed.

11.12 References

Alexander, M (editor). "Guarding Against Computer Calamity." *Infosecurity News*. 4(6), 1993, pp. 26-37.

Coleman, R. "Six Steps to Disaster Recovery." *Security Management*. 37(2), 1993, pp. 61-62.

FitzGerald, J. "Risk Ranking Contingency Plan Alternatives." *Information Executive*, 3(4), 1990, pp. 61-63.

Guidelines for ADP Contingency Planning. FIPS PUB 87. National Institute of Standards and Technology, 1981.

Helsing, C. "Business Impact Assessment." *ISSA Access*. 5(3), 1992, pp. 10-12.

Kabak, I. and T. Beam, "On the Frequency and Scope of Backups." *Information Executive*, 4(2), 1991, pp. 58-62.

Kay, R. "What's Hot at Hotsites?" *Infosecurity News*. 4(5), 1993, pp. 48-52.

Rhode, R. and J. Haskett, "Disaster Recovery Planning for Academic Computing Centers." *Communications of the ACM*. 33(6), 1990, pp. 652-657.

12 Computer Security Incident Handling

12.1 Introduction

Computer systems are subject to a wide range of mishaps -- from corrupted data files, to viruses, to natural disasters. Some of these are fixed through standard operating procedures. For example, frequently occurring events (e.g., a mistakenly deleted file) can usually be readily repaired (e.g., by restoration from the backup file). Other damaging events result from *deliberate malicious technical activity* (e.g., the creation of viruses or system hacking).

The threats posed by hackers and malicious code to systems and networks are well known -- but the occurrence of such harmful events remains unpredictable. Security incidents on larger networks (e.g., the *Internet*) such as break-ins and service disruptions have harmed various organizations' computing capabilities. When initially confronted with such incidents, most organizations respond in an *ad hoc* manner. However recurrence of similar incidents often makes it cost-beneficial to develop a standing capability for quick discovery of and response to such events. This is especially true since, left unchecked, incidents can often "spread," thus increasing damage and seriously harming an organization.

Computer security incidents can range from a single virus occurrence to a hacker attacking many networked systems. An *incident* is mainly used to refer to a computer security problem arising from a technical threat that, left alone, could damage an organization.

This chapter describes how organizations can address computer security incidents (in the context of their larger computer security program) by developing a *computer security incident handling capability*.[50]

12.1.1 Terminology

A computer security incident can result from a computer virus, other malicious code or a system intruder. It is used in this chapter to broadly refer to those incidents resulting from deliberate malicious technical activity.[51] It can more generally refer to those incidents that, without technically-expert response, could result in potentially extreme damage.[52] This definition of a computer security incident is somewhat flexible and may vary by organization

[50] See NIST Special Publication 800-3, *Establishing an Incident Response Capability*, November, 1991.

[51] Some organizations may wish to expand this to include, for example, incidents of theft.

[52] Indeed, damage may result despite the best efforts to the contrary.

and computing environment.

12.1.2 Relationship to Contingency Planning

Incident handling is closely related to contingency planning. An incident handling capability can be viewed as a component of contingency planning,[53] because it provides the ability to react quickly and efficiently to disruptions in normal processing. In this case, incident handling would be that portion of contingency planning that responds to malicious technical threats.

12.2 Benefits of an Incident Handling Capability

The primary benefits of an incident handling capability are:

- *containing* and *repairing* damage from incidents, and
- *preventing* future damage.

In addition there are less obvious side benefits related to establishing an incident handling capability. The following sections discuss these three categories of benefits from an incident handling capability.

12.2.1 Containing and Repairing Damage from Incidents

The first benefit of an incident handling capability is that it provides a means for an organization to contain and repair damage from incidents that occur: viruses, worms, hackers, and so forth. For example, malicious software, when left to spread unchecked, may have the potential to significantly harm an organization's computing, depending on the technology and its connectivity. The response capability provides a way for users to report incidents[54] and the appropriate response and assistance to be provided to aid in recovery. Technical capabilities (e.g., trained personnel and virus identification software) are pre-positioned, ready to be used as necessary. Moreover, the organization will have already made important contacts with other sources (e.g., legal, technical, and managerial) to aid in containment and recovery efforts.

Without an incident handling capability, steps may be taken that can actually make matters worse. In some cases, individuals have unknowingly infected anti-virus software with viruses

[53] Some organizations may not find it useful to make this distinction, but the concepts of availability of important systems provides the connection between the two.

[54] A good incident handling capability is closely linked to an organization's training and awareness program. It will have educated users about such incidents and what to do when they occur. This can increase the likelihood that incidents will be reported early, thus helping to minimize damage.

and then spread them to other systems. When viruses spread to local area networks (LANs), most or all of the connected computers can be infected within hours. Moreover, *uncoordinated* efforts to rid LANs of viruses can prevent their eradication. Some organizations suffer repeated outbreaks of viruses because the viruses are never completely eradicated. For example suppose two LANs, Personnel and Budget, are connected and a virus has spread within each. The administrators of each LAN detect the virus and decide to eliminate the virus on their LAN. The Personnel LAN administrator first eradicates the virus but, since the Budget LAN is not yet virus-free, the Personnel LAN is re-infected. Somewhat later, the Budget LAN administrator eradicates the virus. However, the virus reinfects the Budget LAN from the Personnel LAN. Both administrators may think all is well, but both are reinfected. An incident handling capability allows organizations to address recovery and containment of such incidents in a skilled, coordinated manner.

Many organizations use large LANs internally and also connect to public networks, such as the *Internet*. By doing so, organizations increase their exposure to threats from intruder activity, especially if the organization has a high profile (e.g., perhaps it is involved in a controversial program). Clearly, an incident handling capability can provide enormous benefits by responding quickly to suspicious activity and coordinating incident handling with responsible offices and individuals as necessary. Intruder activity, whether hackers or malicious code, can often affect many systems located at many different network sites; thus, handling the incidents can be logistically complex and require information from outside the organization. By planning ahead, such contacts can be pre-established and the speed of response improved, thereby containing and minimizing damage. Other organizations may also have already had to deal with similar situations and may have very useful guidance to offer in speeding recovery and minimizing damage.

12.2.2 Preventing Future Damage

An incident handling capability also assists an organization in preventing (or at least minimizing) damage from future incidents. Incidents can be studied internally to gain a better understanding of the organizations's threats and vulnerabilities. Additionally, through outside contacts (established by the incident handling capability) early warnings of threats and vulnerabilities can be provided. Mechanisms will already be in place to warn users of these risks.

The incident handling capability allows an organization to learn from the incidents that it has experienced. Data about past incidents (and the corrective measures taken) can be collected. This data can be analyzed for patterns -- for example, which virus are most prevalent, which corrective actions are most successful, and which systems and information are being targeted by hackers. Vulnerabilities can also be identified in this process -- for example, whether damage is occurring to systems when a new software package or patch is used. Knowledge about the types of threats that are occurring and the presence of vulnerabilities can aid in identification of security solutions. This information will also prove useful in the organization's training and awareness program. By educating users, future damage can be

reduced. The incident handling capability can assist in creating a more effective training and awareness program -- and thus help realize reduction in losses. The incident handling capability assists the training and awareness program by providing information to users as to 1) measures which can help avoid incidents (e.g., virus scanning) and 2) what should be done in case an incident does occur.

Of course, the organization's attempts to prevent future losses does not occur in a vacuum. With a sound incident handling capability, ties will have been put in place with counterparts outside the organization. This will allow for *early warning* of threats and vulnerabilities which the organization may have not yet experienced. Early preventative measures (generally more cost-effective than repairing damage) can be taken to reduce future losses. Data is also shared outside the organization to allow others to learn from the organization's experiences.

12.2.3 Side-Benefits

Finally, establishing an incident handling capability helps an organization in perhaps unanticipated ways. Three are discussed below.

12.2.3.1 Uses of Threat and Vulnerability Data

Incident handling can greatly enhance the risk assessment process. An incident handling capability will allow organizations to collect threat data that may be useful in their risk assessment and safeguard selection processes (e.g., in designing new systems). Incidents can be logged and analyzed to determine whether there is a recurring problem (or if other patterns are present, as are sometimes seen in hacker attacks), which would not be noticed if each incident were only viewed in isolation. Statistics on the numbers and types of incidents in the organization can be used in the risk assessment process as an indication of vulnerabilities and threats.[55]

12.2.3.2 Enhancement of Internal Communications and Organization Preparedness

Also, organizations often find that an incident handling capability enhances internal communications and the readiness of the organization to respond to any type of incident, no matter the source. Internal communications will be improved; management will be better organized to receive communications; and contacts within public affairs, legal staff, law enforcement, and other groups will have been pre-established. The structure set up for reporting incidents can also be used for other purposes.

12.2.3.3 Enhancing the Training and Awareness Program

[55] It is important, however, *not* to assume that since only *n* reports were made, that *n* is the total number of incidents; it is likely that not all incidents will ever be reported.

The organization's training process can also benefit from incident handling experiences. Based on incidents reported, training personnel will allow a better understanding of user's knowledge of security issues. Actual incidents can be used to vividly illustrate the importance of computer security. Training that is based on current threats and controls recommended by incident handling staff provides users with information more specifically directed to their current needs -- thereby reducing the risks to the organization from incidents.

12.3 Characteristics of a Successful Incident Handling Capability

There are several core characteristics of a successful incident handling capability, namely:

- an understanding of the scope and of the constituency that the incident handling capability will serve;
- a means for centralized communications;
- expertise in the requisite technologies; and
- links to other groups to assist in incident handling (as needed).

Each of these concepts is discussed below.

12.3.1 Defining the Constituency to be Served

The constituency includes those computer users and program managers to be served by the incident handling capability. Like any other customer-vendor relationships, the constituency will tend to take advantage of the capability if the services rendered are valuable.

The constituency is not always the entire organization. For example, an organization might utilize several types of computers and networks but may decide that its incident handling capability is cost-justified only for its personal computer users. In doing so, it may have determined that computer viruses pose a much larger risk to the organization than other malicious technical threats on other platforms. Or, a large organization composed of several sites may decide that current computer security efforts at some sites do not require an incident handling capability, whereas other sites do (perhaps because of the criticality of processing).

12.3.2 Centralized Reporting and Communications

Successful incident handling requires that users be able to report incidents to the incident handling team in a convenient, straightforward fashion; this is referred to as *centralized reporting*. A successful incident handling capability depends on timely incident reporting. If it is made difficult or time consuming to report incidents, the incident handling capability may not be fully utilized. Usually, some form of a hotline, backed up by pagers, suffices well.

Centralized communications is very useful as a means of accessing or distributing information relevant to the incident handling effort. For example, if users are linked together via a network, the incident handling capability can then use the network to send out announcements and other information in a timely manner. Users can take advantage of the network to retrieve security information stored on servers and communicate with the incident response team via e-mail.

Encouraging users to report incidents may present dilemmas for security managers. Reporting may be unintentionally discouraged if users fear reprisal or that they will become scapegoats. At the same time, managers need to know details about incidents, including who discovered them and how, so that similar incidents can be prevented in the future. Organizations may need to offer incentives to employees for reporting incidents and offer guarantees against reprisal or other adverse actions. It may also be useful to consider anonymous reporting.

12.3.3 Technical Platform and Communications Expertise

The technical staff members who comprise the incident handling capability require appropriate knowledge, skills and abilities. Technical expertise in the constituency's technology is essential; however, it is often desirable that this be supplemented by broader non-technical skills. Sound communications skills are also a necessity. Desirable qualifications for technical staff members may include:

- facility with some or all of the constituency's core technology;
- ability to work in a group environment;
- ability to communicate effectively with different types of users, who will range from system administrators to unskilled users to management to law-enforcement officials;
- availability on-call 24 hours as needed; and
- ability to travel on short notice (of course, this depends upon the physical location of the constituency to be served).

12.3.4 Liaison with Other Organizations

Due to the increasing computer connectivity, intruder activity on networks can affect many organizations, sometimes including those in foreign countries. Therefore, an organization's incident handling team may need to work with other teams or security groups to effectively handle incidents that range beyond its constituency. Additionally, the team may need to pool its knowledge with other teams at various times. Thus, it is vital to the success of an incident handling capability that it establish ties and contacts with other related counterparts and supporting organizations.

Especially important to incident handling are contacts with investigative agencies such as federal (e.g., the FBI), state, and local law enforcement. Laws that affect computer crime vary among localities and states, and some actions may be state (but not federal) crimes. It is important for teams to be familiar with current laws and to have established contacts within law enforcement and investigative agencies.

The Forum of Incident Response and Security Teams

Beginning with the aftermath of the 1988 *Internet* worm incident, it was recognized that better methods for incident response and information sharing were needed. It was also clear that any single team or "hot line" would simply be overwhelmed. Out of this was born the concept of a coalition of response teams -- each with its own constituency, but working together to share information, provide alerts, and support each other in the response to incidents. The Forum of Incident Response and Security Teams (FIRST) includes teams from government, industry, computer manufacturers, and academia. NIST serves as the secretariat of FIRST.

Incidents can also garner much media attention and can reflect quite negatively on an organization's image. An incident handling capability may need to work closely with the organization's public affairs office, which is trained in dealing with the news media. In presenting information to the press, it is important that 1) attackers are not given information that would place the organization at greater risk and 2) potential legal evidence is properly protected.

12.4 Technical Support for Incident Handling

Incident handling will be greatly enhanced by technical mechanisms that enable the dissemination of information quickly and conveniently. This section details such technical support mechanisms for incident handling.

12.4.1 Communications for Centralized Reporting of Incidents

The technical ability to report incidents is of primary importance, since without knowledge of an incident, response is precluded. Fortunately, such technical mechanisms are already in place in many organizations.

For rapid response to constituency problems, a simple telephone "hotline" is practical and convenient. Some agencies may already have a number used for emergencies or for obtaining help with other problems; it may be practical (and cost-effective) to also use this number for incident handling. It may be necessary to provide 24-hour coverage for the hotline. This can be done by either staffing the answering center, by providing an answering service for non-office hours, or by using a combination of an answering machine and personal pagers.

If additional mechanisms for contacting the incident handling team can be provided, it may increase access and thus benefit incident handling efforts. A centralized e-mail address that forwards mail to staff members would permit the constituency to conveniently exchange information with the team. Providing a fax number to users may also be helpful.

12.4.2 Rapid Communications Facilities

A simple 24-hour telephone hotline is often practical and convenient for incident reporting. Often, such numbers exist for other purposes and costs can be minimized by avoiding duplication of effort.

Some form of rapid communications is essential for quickly communicating with the constituency as well as management officials and outside organizations. The team may need to send out security advisories or collect information quickly, thus some convenient form of communications, such as electronic mail, is generally highly desirable. With electronic mail, the team can easily direct information to various sub-groups within the constituency, such as system managers or network managers, and broadcast general alerts to the entire constituency as needed. When connectivity already exists, e-mail has low overhead and is easy to use.

Substitutes for rapid communications exist (e.g., flyers or physical bulletin boards) but tend to reduce response time. An electronic bulletin board system (BBS) can work well for distributing information, especially if it provides a convenient user interface that encourages its use. A BBS connected to a network is more convenient to access than one that requires use of a terminal and modem; however, the latter may be the only alternative for organizations without sufficient network connectivity.

12.4.3 Secure Communications Facilities

Secure communications can help protect against unintended distribution of incident-related information.

Incidents can range from the trivial to those involving national security. Often when communicating information about incidents use of encrypted communications may be advisable. This will help prevent others from exploiting known vulnerabilities. Encryption technology is available for voice, fax, and e-mail communications.

12.5 Interdependencies

An incident handling capability generally depends upon other safeguards presented in this Handbook. The most obvious is the strong link to other components of the Contingency Plan. The following paragraphs detail the most important of these interdependencies.

Contingency Planning. As discussed in the introduction to this chapter, an incident handling capability can be viewed as the component of contingency planning that deals with responding to technical threats, such as viruses or hackers. Close coordination is necessary with other contingency planning efforts, particularly when planning for use of contingency processing in the event of a serious unavailability of system resources.

Support and Operations. Incident handling is also closely linked to support and operations.

For example, for purposes of efficiency and cost savings, the incident handling capability is often co-operated with a user "help desk." Also, backups of system resources may need to be used when recovering from an incident.

One way to establish a centralized reporting and incident response capability, while minimizing expenditures, is to utilize an existing **Help Desk**. Many agencies already have central help desks for fielding calls about commonly used applications, troubleshooting system problems, and providing help in detecting and eradicating computer viruses. By expanding the capabilities of the help desk and publicizing its telephone number (or e-mail address), an agency may be able to significantly improve its ability to handle many different types of incidents at minimal cost.

Training and Awareness. The training and awareness program can benefit from lessons learned during incident handling. Incident handling staff members will be able to help assess the level of user awareness of current threats and vulnerabilities. Staff members may be able to help train system administrators, system operators, and other user and systems personnel. Knowledge of security precautions (resulting from such training) helps reduce future incidents.

Risk Management. The risk analysis process will benefit from statistics and logs on the numbers and types of incidents that have occurred, and the types of controls that are effective to prevent incidents from recurring. This information can be used to help in the selection of appropriate security controls and practices.

12.6 Cost Considerations

There are a number of start-up costs and funding issues to consider when planning an incident handling capability. Because the success of an incident handling capability relies so heavily on users' perceptions of its worth and whether they use it, it is very important that an incident handling capability be able to meet users' requirements. The following are two of the important funding issues.

Personnel. An incident handling capability plan might call for at least one manager and one or more technical staff members (or their equivalent) to accomplish program objectives. Depending on the scope of the effort, however, full-time staff members may not be required. In some situations, some staff may be needed part-time or on an on-call basis. Full-time staff may be performing incident handling duties as an adjunct responsibility to their normal assignment.

Education and Training. Incident handling staff will need to keep current with computer system and computer security developments. Budget allowances need to be made, therefore, for attending conferences, security seminars, and other continuing education-related events. If an organization is located in more than one geographic locations, funds will probably be needed for travel to other sites for handling incidents.

12.7 Summary

An incident handling capability provides a useful mechanism for organizations to address malicious technical threats such as viruses or hacker activity. This capability can decrease response time, strengthen security and reduce exposure to technical vulnerabilities. Establishing an incident handling capability requires knowledge of the type and scope of the constituency to be served and developing the technical and managerial mechanisms to provide the incident handling support.

12.8 References

Brand, Russell L. *Coping With the Threat of Computer Security Incidents: A Primer from Prevention through Recovery*. July, 1989.

Computer Security - Virus Highlights Need for Improved Internet Management. United States General Accounting Office, 1989.

Fedeli, Alan. "Organizing a Corporate Anti-Virus Effort." *Proceedings of the Third Annual Computer VIRUS Clinic*, Nationwide Computer Corp., March, 1990.

Holbrook, P., and Reynolds, J. *Security Policy Handbook*, RFC 1244 prepared for the Internet Engineering Task Force, 1991.

Padgett, K. *Establishing and Operating an Incident Response Team*. Los Alamos National Laboratory, 1992.

Pethia, Rich, and van Wyk, Kenneth. *Computer Emergency Response - An International Problem*. 1990.

Quarterman, John. *The Matrix - Computer Networks and Conferencing Systems Worldwide.* Digital Press, 1990.

Scherlis, William, Squires, Steven, and Pethia, Rich. *Computer Emergency Response*. 1989.

Schultz, E. Eugene, Brown, David, and Longstaff, Thomas. *Responding to Computer Security Incidents: Guidelines for Incident Handling*. University of California Technical Report UCRL-104689, 1990.

Proceedings of the Third Invitational Workshop on Computer Security Incident Response. August, 1991.

Wack, John. *Establishing an Incident Response Capability*. Spec. Pub. 800-3. National Institute of Standards and Technology. November, 1991.

13 Awareness, Training, and Education

13.1 Introduction

Computer security awareness, training, and education seeks to enhance security by changing people's behavior.[56] People, who are fallible, are usually recognized as one of the weakest links in securing systems. Improving human behavior may include decisions made by a manager, the actions of a computer system user, or the design work of a systems engineer. The purpose of computer security awareness, training, and education is to improve:

- awareness of the need to protect system resources;
- skills and knowledge so computer users can perform their jobs while furthering computer security; and
- in-depth knowledge, as needed, to design, implement or operate security programs for organizations and systems.

Making computer system users aware of their security responsibilities and teaching them correct practices also augments realization of *individual accountability*, which is one of the most important ways to improve computer security. Without knowing the necessary security measures (and to how to use them), users cannot be truly accountable for their actions. The importance of this was emphasized in the Computer Security Act which requires such training for those involved with the management, use, and operation of federal computer systems.

This chapter first discusses the two overriding benefits of awareness, training, and education, namely improving employee behavior and increasing the ability to hold employees' accountable for their actions. Next, awareness, training, and education are discussed, separately, including techniques used for each. Finally, the chapter presents one approach for developing a computer security awareness and training program.[57]

13.2 Behavior

People are a crucial factor in ensuring the security of computer systems and valuable information resources. Human actions account for a far greater amount of computer-related loss than all other sources combined. Of such losses, the actions of an organization's

[56] One often cited goal of training is changing peoples' attitudes. This chapter views changing attitudes as just one step toward changing behavior.

[57] This chapter does not discuss the specific contents of training programs. See the references for details of suggested course contents.

employees and contractors normally cause far more harm than that of outsiders. (The Threat Chapter discusses the major sources of computer-related loss.) The major causes of loss by an organization's own employees are: errors and omissions, fraud, and actions by disgruntled employees. One principal purpose of security awareness, training, and education is to reduce errors and omissions. However, it can also reduce fraud and unauthorized actions by disgruntled employees by increasing employee's knowledge of their accountability and the penalties associated with such actions.

Before moving on to the rest of the chapter, it is necessary to put awareness, training, and education programs in the proper context with other programs that affect employee behavior. *Management sets the example for behavior within an organization.* If employees know that management does not really care about security, no training class teaching the importance of security and imparting valuable skills can be truly effective.

13.3 Accountability

Computer security awareness and training is a primary mechanism for teaching people about organizational policy and the procedures to be followed to implement policy. As discussed in the Policy Chapter, both the *dissemination* of policy and the *enforcement* of policy are critical issues -- which are implemented and strengthened through training programs. Employees cannot be expected to follow policies and procedures of which they are unaware. In addition, it may be difficult to enforce penalties if users can claim ignorance when they are caught doing something wrong.

Training employees may also be necessary to show that a standard of *due care* has been taken in protecting information. Simply issuing policy, with no follow-up to implement that policy, may not suffice.

> One of the keys to a successful computer security program is security awareness and training. If employees are not informed of applicable organizational policies and procedures they cannot be expected to act effectively to secure computer resources.

Many organizations use *acknowledgement statements* which state that employees have read and understand computer security requirements and agree to abide by them. (See the example provided in the Personnel/User Issues chapter.)

Next, awareness, training, and education are each discussed.

13.4 Awareness

The purpose of awareness is to stimulate and motivate those being trained to care about security and to remind them of important security practices. Motivating people is normally performed by informing them about the importance of security, often by explaining what happens if security fails.

Awareness can take on different forms for particular audiences. Appropriate awareness for management might stress its pivotal role in establishing organizational attitudes toward security. Appropriate awareness for other groups, such as system programmers or information analysts, should address the need for security as it relates to their job. In today's systems environment almost everyone in an organization may have access to system resources -- and therefore may have the potential to cause harm.

> Security *awareness* programs: 1) set the stage for *training* by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure; and 2) remind users of the importance of security and the procedures to be followed.

Awareness is used to reinforce the fact that security supports the mission of the organization by protecting valuable resources. If employees view security as just a group of bothersome rules and procedures, they are more likely ignore or avoid them. In addition, they may not make needed suggestions about improving security nor recognize and report security threats and vulnerabilities.

Awareness also is used to remind people of basic security practices, such as logging off a computer system or locking doors.

> Employees often regard computer security as an obstacle to productivity. A common feeling is that they are paid to produce, not to protect. To help motivate employees, awareness should emphasize how security, from a broader perspective, contributes to productivity. The consequences of poor security should be explained while avoiding the fear and intimidation often associated with security by employees.

Techniques. A security awareness program can use many teaching methods including video tapes, newsletters, posters, bulletin boards, flyers, demonstrations, briefings, short reminder notices at logon, talks, or lectures. Awareness is often incorporated into basic security training and can use any method that can change employees' attitudes. Security awareness should also be built into existing organizational information practices.

Effective security awareness programs must be designed with the recognition that people tend to practice a *tuning out* process (also known as *acclimation*). For example, after a while, a security poster, no matter how well designed, will be ignored; it will, in effect, simply blend into the environment. For this reason, awareness techniques must be frequently changed. Awareness programs must be ongoing and creative.

13.5 Training

The purpose of training is to teach people the skills that will enable them to perform their jobs more securely. This includes teaching people *what* they should do and *how* they should (or can) do it. Training can address many levels including basic security practices and more advanced or specialized skills. It can be specific to one computer system or generic enough

to address all systems.

Training is most effective when targeted to a specific audience. Two primary audiences are general users and those who require specialized or advanced skills.

General Users. Most users need to understand good computer security practices such as:

- protection of the physical area and equipment (e.g., locking doors, care of floppy diskettes);
- protection of passwords (if used) or other authentication data or tokens (e.g., never divulge PINs); and
- reporting of security violations or incidents (e.g., who to call if a virus is suspected).

In addition, general users should also be taught the organization's policies for protecting information and computer systems and the roles and responsibilities of various organizational units with which they may have to interact.

Care should be taken in teaching general users not to overburden them with unneeded details. The same people are the target of multiple training programs, such as safety, sexual harassment, or AIDS in the workplace. The training should be useful, especially by addressing security issues that *directly* affect the users. The goal is to improve basic security practices *not* to make everyone literate in all the jargon or philosophy of security.

Specialized or Advanced Training. Many groups of people need more advanced or specialized training than just basic security practices. This could include managers who need to understand security consequences and costs so they can factor security into their decisions or system administrators who need to know how to implement and use specific access control products.

There are many different ways to identify individuals or groups who need specialized or advanced training. One method is to look at job category, such as executives, functional managers, or technology providers. Another method is to look at job function, such as system design, system operation, or system user. A third method is to look at the specific technology and products used, especially for advanced training for user groups and training to use a new system. This is further discussed in the Implementation Section below.

Techniques. A security training program normally includes training classes, either those devoted to security or by adding security modules to existing training classes. Training can be computer- or lecture-based (or both), and may include hands-on practice and case studies. Training, like awareness, also happens on-the-job.

13.6 Education

Security education is more in-depth than security training. It is targeted for security professionals and those whose jobs require *expertise* in security.

One group that has been targeted for specialized training is executives and functional managers. As discussed in this chapter, without management support or security, employee support is likely to be unobtainable. The training for management personnel is specialized (rather than advanced) because managers do *not* (as a general rule) need to understand the technical details of security. However, they do need to understand how to organize security, how to direct and evaluate security, security costs, and what it means to accept risk.

Techniques. Security education is normally outside the scope of most organization awareness and training programs. It is more appropriately a part of *employee development*. Security education is implemented through college or graduate classes or through specialized training programs. Because of its highly specialized nature, most computer security programs focus primarily on awareness and training, as is done in the remaining portion of this chapter.

13.7 Implementation[58]

An effective computer security awareness and training (CSAT) program requires proper planning, implementation, maintenance, and periodic evaluation. The following steps are *one approach for developing a CSAT program.*

Step 1: Identify Program Scope, Goals, and Objectives

Step 2: Identify Training Staff

Step 3: Identify Target Audiences

Step 4: Motivate Management and Employees

Step 5: Administer the Program

Step 6: Maintain the Program

Step 7: Evaluate the Program

13.7.1 Identify Program Scope, Goals, and Objectives

The first step in developing a CSAT program is to determine the program's scope, goals and

[58] This section is based on material prepared by the Department of Energy's Office of Information Management for their unclassified security program.

objectives. The scope of the CSAT program should be designed to provide training to all types of people who interact with computer systems. The scope of the program can be an entire organization or a subunit. The scope should specifically address whether the program applies to employees only or also to other users of organization systems.

> The Computer Security Act of 1987 requires federal agencies to "provide for the mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency." The scope and goals of federal computer security awareness and training programs must implement this broad mandate.

Generally, the overall goal of a CSAT program is to sustain an appropriate level of protection for computer resources by increasing employee awareness of their computer security responsibilities and the ways to fulfill them. More specific goals may need to be established. Objectives should be defined to meet the organization's specific goals.

13.7.2 Identify Training Staff

Who should actually run the training? There are many possible alternatives, including internal training departments, computer security staff, of contract services. Whoever is chosen to provide the training, it is important that they have sufficient knowledge of computer security issues. It is also vital that they know how to communicate information and ideas effectively.

13.7.3 Identify Target Audiences

Not all individuals require the same degree or type of computer security information to perform their jobs. A CSAT program that distinguishes between groups of people and presents the information truly needed by the particular audience and omits irrelevant information will have the best results. Segmenting audiences (e.g., by their function or familiarity with the system) can also maximize the effectiveness of a CSAT program. For larger organizations, some individuals will fit into more than one group. For smaller organizations, segmenting may not be needed. The following methods are some examples of ways to do this.

Segment according to level of awareness. Individuals may be separated into groups according to their level of awareness. This can include research to determine how well employees follow computer security procedures or how well employees understand the objective of computer security associated with their jobs.

Segment according to general job task or function. Individuals could be grouped as data providers, data processors, or data users.

Segment according to specific job category. Many organizations assign individuals to job

categories. Since each job category generally has different job responsibilities, training for each will be different. Examples of job categories could be general management, technology management, applications development, or security officers.

Segment according to level of computer knowledge. Computer "experts" would obviously find a program containing highly technical information more valuable than one covering the fundamentals of computer security. Similarly, a computer novice would benefit more from a training program that discussed the fundamentals.

Segment according to types of technology or systems used. Security techniques used for each off-the-shelf product or application system will usually vary.

13.7.4 Motivating Management and Employees

To successfully implement an awareness and training program, it is important to gain the *support* of management and employees. Consideration should be given to using motivational techniques to convince management and employees that their participating in the CSAT program will be beneficial to the organization.

Management. Motivating management is primarily an awareness issue. Management needs to be aware of the losses that computer security can reduce and the role of training in computer security. Management commitment is necessary because of the expenditure of resources used in developing and implementing the program and also because the program affects their employees.

Employees. Motivation of management personnel alone is not enough. Employees often need to be convinced of the merits of computer security and how it relates to their jobs. Without appropriate training, many employees will not fully comprehend the value of the system resources with which they work.

> Employees should be solicited to provide input to the CSAT program. Employees are more likely to support a program when they have actively participated in its development.

Some awareness techniques were discussed above. Regardless of the techniques that are used, employees must feel that their cooperation will have a beneficial impact on the organization's future (and, consequently, their own).

13.7.5 Administer the Program

There are several important considerations for administering the CSAT program.

Visibility. The visibility of a CSAT program plays a key role in its success. Efforts to achieve a high degree of visibility should begin during the early stages of CSAT program

development.

Selection of Training Methods. The methods used in the CSAT program should be consistent with the material presented and tailored to the audience's needs. Some training and awareness methods and techniques are listed above. Consideration should also be given to on-the-job training.

The Federal Information Systems Security Educators' Association and NIST Computer Security Program Managers' Forum provide a means for federal government computer security program managers and training officers to share training ideas and materials.

Selection of Training Topics. There are more topics in computer security than can be taught in any one course. Topics should be selected based on the audience's requirements and prioritized to maximize impact.

Selection of Training Materials. In general, higher quality the training materials are more favorably received and are more expensive. Costs, however, can be minimized since training materials can often be obtained from other organizations.

Training Presentation Techniques. Consideration should be given to the frequency of training (e.g., annually, as needed, continuous), the length of training presentations (e.g., twenty minutes for general presentations, one hour for updates or one week for an off-site class), and the style of training presentation (e.g., formal presentation, informal discussion, humorous).

13.7.6 Maintain the Program

Efforts should be made to keep abreast of changes in computer technology and security requirements. Computer technology is an ever-changing field. A training program that meets all necessary requirements may become ineffective if the organization receives new computer equipment or software. Likewise, an awareness program can become obsolete if laws or organization policies change.

13.7.7 Evaluate the Program

It is often difficult to measure the effectiveness of an awareness or training program; however, an evaluation should attempt to ascertain how much information is retained, to what extent computer security procedures are being followed, and general attitudes towards computer security. The results of an evaluation should help identify and correct problems. Some evaluation methods (which can be used in conjunction with one another) are:

- Use of student evaluations;
- Observe how well employees follow recommended security procedures;
- Test employees on material covered; or

- Monitor the number and kind of computer security incidents reported before and after the program is implemented.[59]

13.8 Interdependencies

Training can, and in most cases should, be used to support every control in the Handbook. All controls are more effective if designers, implementers, and users are adequately trained. However, policy, in particular, relies upon training:

> *Policy*. Training is a critical means of informing employees of the contents of and reasons for the organization's policies.

13.9 Cost Considerations

The major cost considerations in awareness, training, and education programs are:

- the cost of preparing materials, including the time of the preparer;
- the cost of those providing the instruction;
- employee time attending courses, lectures, or watching videos; and
- the cost of outside courses and consultants (both of which may including travel expenses).

13.10 Summary

A security awareness, training, and education program can play a valuable role in the protection of an organization's system resources. It does so by explaining organizational policies, the reasons they were adopted, and teaches specific skills necessary to implement them. The program also helps ensure accountability of computer users. Many techniques can be used to implement the program and target it toward specific groups of users.

13.11 References

Alexander, M. (editor) "Multimedia Means Greater Awareness." *Infosecurity News*, 4(6), 1993. pp. 90-94.

[59] Note that the number of incidents will not necessarily go down. For example, virus-related losses may decrease when users know the proper procedures to avoid infection. On the other hand, reports of incidents may go up as users will be employing virus scanners and finding more viruses. In addition, users will now know that virus incidents should be reported and to whom the reports should be sent.

Burns, G.M. "A Recipe for a Decentralized Security Awareness Program." *ISSA Access*. Volume 3, Issue 2, 2nd Quarter 1990, pp. 12-54.

Computer Security Awareness and Training Guideline. U.S. Department of Energy. DOE/MA-0320 (Vol. 1). February, 1988.

Flanders, D. "Security Awareness - A 70% Solution" Fourth Workshop on Computer Security Incident Handling, August 1992.

Guidelines for Development of Computer Security Awareness and Training (CSAT) Programs. NASA Guide 2410.1. National Aeronautics and Space Administration. March 1990.

Isaacson, G. "Security Awareness: Making It Work," *ISSA Access*, 3(4), 1990. pp. 22-24.

Maconachy, V. "Computer Security Education, Training, and Awareness: Turning a Philosophical Orientation Into Practical Reality." *Proceedings of the 12th National Computer Security Conference*. October 1989.

Maconachy, V. "Panel: Federal Information Systems Security Educators' Association (FISSEA)." 15th National Computer Security Conference, October 15, 1992.

Suchinsky, A. "Determining Your Training Needs." *Proceedings of the 13th National Computer Security Conference*, October 1990.

Todd, M.A. and Guitian C. *"Computer Security Training Guidelines*." Spec. Pub. 500-172. NIST, November 1989.

Wells, R.O. "Security Awareness for the Non-Believers." *ISSA Access*, Volume 3, Issue 2, 2nd Quarter 1990, pp. 10-61.

14 Security Considerations in Computer Support & Operations

14.1 Introduction

Computer support and operations is a hard term to define. It refers to all the things that are done to run a computer system and to run it well. This includes both system administration and tasks that are external to the system but also support its operation. It does not include planning or designing systems.

The support and operation of any computer system, from a three-person local area network to a world-wide application serving thousands of users, is critical to maintaining the security of a system. *Support and operations* comprise the routine activities that enable computer systems to function correctly, such as fixing software or hardware problems, loading and maintaining software, or helping users resolve problems. The tasks are generally performed by system management and administration staff, but sometimes by users. Larger systems may have full-time operators, system programmers, and support staff performing these tasks. Smaller systems may have a part-time administrator.

This chapter addresses the support and operations activities directly related to security. Every control discussed in this Handbook relies, in one way or another, on computer system support and operations. This chapter, however, focuses on areas *not covered in other chapters*. For example, operations personnel normally are those who actually create user accounts on the system. This topic is covered in the Identification and Authentication Chapter, so it is not discussed here. Similarly, the input from support and operations staff to the security awareness and training program is covered in the Security Awareness, Training, and Education Chapter.

Failure to consider security as part of the support and operations of computer systems is, for many organizations, their Achilles' heel. Computer security system literature includes many examples of how organizations undermined their own, often expensive, security measures because of poor documentation, conflicting software, or poor control of computer accounts for maintenance purposes. Also, policy often fails to address many of these important issues.

Since the primary goal of computer support and operations is the continued and correct operation of a computer system, and one of the goals of computer security is the availability and integrity of systems, these areas are very closely linked. This chapter focuses on areas of support and operations with *special* security concerns that are not discussed elsewhere in this Handbook.

This chapter discusses some of the many tasks within support and operations that have significant security considerations. Each of these activities is primarily performed for support and operations -- *not* for security. The important security considerations within some of the major categories of support and operations are:

User Support - to help users understand when they may have a security problem and

what actions they should take;

Software Support - to check that software security controls cannot be subverted and that software is protected from unauthorized modification;

Configuration Management - to ensure that changes to the system do not unintentionally or unknowingly diminish security;

Backups - to ensure that data and programs are available in case of a contingency;

Media Controls - to prevent the loss of confidentiality, integrity, or availability of data when stored outside the system;

Documentation - to ensure that security-relevant documentation is up-to-date and accessible;

Maintenance - to ensure that security breaches do not occur through various maintenance procedures and that maintenance itself does not harm security;

These areas may have *special considerations* for larger or smaller systems, which are noted appropriately. In general, larger systems include mainframes, large minicomputers, and WANs. Smaller systems include PCs and LANs.

14.2 User Support

Of specific concern in this chapter is the interaction between systems personnel and users as a component of user support. In many organizations, this takes place through a *Help Desk*. Help desks can support an entire organization or a specific system. For smaller systems, user support is normally provided directly by the system administrator. Informal user support on most systems is provided by other users (usually those who are more experienced or technically inclined).

> User support should be closely linked to the organization's incident handling capability. In many cases, these functions will be performed by the same personnel.

An important security consideration for user support personnel is being able to recognize which problems (brought to their attention by users) are security-related. For example, a user's inability to log onto a computer system may result from the disabling of their account due to too many failed access attempts. This could indicate the presence of hackers guessing the user's password.

In general, system support and operations staff need to be able to identify security problems, respond appropriately, and inform appropriate individuals. A wide range of possible security problems exist. Some will be internal to custom applications and others to off-the-shelf products. Additionally, problems can be software or hardware based.

The more responsive and knowledgeable that system support and operation staff personnel are, the less user support will be provided informally by other users. The support provided by other users is important, but they may not be aware of the "whole picture."

Special considerations for small systems: Small systems are especially susceptible to viruses. Support personnel must know how to recognize viruses. (Recovery may be performed by support staff or a separate incident handling staff.)

Special considerations for networks: Networks are especially susceptible to hacker attacks, which can be targeted at multiple systems. System support personnel should be able to recognize attacks.

14.3 Software Support

Software is the heart of an organization's computer operations, whatever the size and complexity of the system. It is therefore essential that software function correctly and be protected from corruption. There are many elements of software support.

One of the elements of software support is *controlling what software is used on a system*. If users or systems personnel can load and execute any software on a system, the system is more vulnerable to viruses, to unexpected software interactions, and to software which may subvert or bypass security controls. As part of this control process, security or systems personnel may inspect or test software before it is loaded (e.g., to determine compatibility with custom applications or identify other unforeseen interactions). This can apply to new software packages or to upgrades, to off-the-shelf products or to custom software. In addition to controlling the loading and execution of new software, care must also be given to the configuration and use of powerful system utilities. System utilities can compromise the integrity of operating systems and logical access controls.

A second element in software support is ensuring that *software has not been modified without proper authorization*. This involves the protection of software on the system and their backup copies. This can be done with a combination of logical and physical access control.

Many organizations also include as an element of software support a program to ensure that no stolen software is run (i.e., illegal copies of copyrighted software). This problem is primarily associated with Pcs and LANs but can apply to any type of system.

Special considerations for smaller systems: Viruses take advantage of the weak software controls in personal computers. Also, there are powerful utilities available for PCs which can restore deleted files, find hidden files, and interface directly with PC hardware, bypassing the operating system.

Special considerations for networks: There are several widely available utilities which look for security problems in both networks and the systems attached to them.

14.4 Configuration Management

Even if configuration management is performed informally, system support personnel should know what changes are made to support contingency planning.

Closely related to software support is *configuration management*. Configuration management is the process of keeping track of changes to the system and, if needed, approving them. Configuration management normally addresses hardware, software, networking, and other changes. Configuration management can be formal or informal. The primary security consideration of configuration management is to ensure that changes to the system do not unintentionally or unknowingly diminish security. Some of the methods discussed under software support, such as inspecting and testing software changes can be used. The Assurance Chapter discusses other methods.

Note that the security goal is to know what changes occur, not to prevent security from being changed. There may be circumstances when security will be reduced.

Special considerations for networked systems: Configuration management should include external connections. Is the computer system connected? To whom? In turn, to whom are *they* connected?

14.5 Backups

Backing up software and data is performed by both support and operations personnel and, for small systems, by users. This function is critical to contingency planning. Frequency of backups will depend upon how often data changes and how important those changes are. Program managers should be consulted to determine what backup schedule is appropriate. Also, as a safety measure, it is useful to test that backup copies are actually usable. Finally, backups should be stored securely, as appropriate (discussed below).

14.6 Media Controls

Media controls include a variety of measures to provide physical and environmental protection and accountability for tapes, diskettes, printouts, and other media. From a security perspective, media controls should be designed to prevent the loss of confidentiality, integrity, or availability of information, including data or software, when stored outside the system. This can include storage of information before it is input to the system and after it is output.

The extent of media control depends upon many factors including the type of data, the quantity of media, and the nature of the user environment. Physical and environmental protection is used to prevent unauthorized individual from accessing the media. It also protects against such factors as heat, cold, or magnetism. When necessary, logging use of individual media (e.g., a tape reel) provides detailed accountability -- to hold authorized people responsible for their actions.

14.7 Marking

Controlling media may require some form of physical labeling. The labels can be used either to identify media with special handling instructions and locate needed information or may be used for logging the media (e.g., serial/control numbers and bar codes) to support accountability. Identification is often performed by colored labels on diskettes or tapes or banner pages on printouts.

Typical markings for media could include: Privacy Act Information, Company Proprietary, or Joe's Backup Tape. In each case the individuals handling the media must know the applicable handling instructions. For example, at the Acme Patent Research Firm, proprietary information cannot leave the building except under the care of a security officer. Also, Joe's backup tape should be easy to find in case something happens to Joe's system.

If labeling is used to support special handling instructions, it is critical that people be appropriately trained.

Special considerations for smaller systems: The marking of PC input and output is generally the responsibility of the *user*, not the system support staff. Marking can be useful for these systems since they often are used to process important information. Marking backup diskettes is also critical so that they are not accidentally overwritten.

14.7.1 Logging

The logging of media is used to support accountability. Logs can include control numbers (or other tracking mechanism), the times and dates of transfers, names and signatures of individuals involved, and other relevant information. Periodic spot checks or audits may be conducted to determine that no controlled items have been lost and that all are in the custody of individuals indicated in control logs. Automated media tracking systems may be helpful for maintaining inventories of tape and disk libraries.

14.7.2 Integrity Verification

When electronically-stored information is read into a computer system, it may be desired to determine whether it has been read correctly or subject to any modification. The integrity of electronic information can be verified using cryptographic-based technologies. (See the Cryptography chapter.)

14.7.3 Physical Access Protection

Physical access is discussed in the Physical and Environmental Controls Chapter.

Media can be stolen, destroyed, replaced with a look alike copy, or lost. Physical access controls to the media, which can limit these problems, include locked doors, desks, file cabinets, or safes.

If the media requires protection at all times, it may be necessary to actually output data to the media in a secure location (e.g., printing to a printer in a locked room instead of to a general purpose printer in a common area).

Physical protection of media should be extended to backup copies stored off-site. They generally should be accorded an equivalent level of protection to media containing the same information stored on-site.

14.7.4 Environmental Protection

Magnetic media, such as diskettes or magnetic tape, require environmental protection since they are sensitive to temperature, liquids, magnetism, and smoke and dust. Other media (e.g., paper and optical storage) may be have different sensitivities to such environmental factors.

14.7.5 Transmittal

Transfer of control of media may occur both within the organization and to outside elements Possibilities for securing such transmittal may include:

- Sealed and marked envelope,
- Authorized messenger or courier, or
- U.S. certified or registered mail.

14.7.6 Disposition

When media is disposed of, it may be important to ensure that information is not improperly disclosed. This applies both to media that is *external* to a computer system (such as a diskette) and to media *inside* a computer system, such as a hard disk. The process of removing information from media is called *sanitization.*

Many people throw away old diskettes believing that erasing the files on the diskette has made the data unretrievable. In reality, however, erasing a file simply removes the pointer to that file. The pointer tells the computer where the file is physically stored. Without this pointer, the files will not appear on a directory listing. This does *not* mean that the file was removed. Commonly available utility programs can often retrieve information that is presumed deleted.

Three techniques are commonly used for media sanitization: overwriting, degaussing, and destruction. *Overwriting* is an effective method of clearing data from magnetic media. As the name implies, overwriting utilizes a program to write (1s, 0s, or a combination) onto the media. The number of times that the media is overwritten depends on the level of sensitivity of the information. Overwriting should not be confused with merely deleting the pointer to a file (which typically happens when an *erase* or *delete* command is used). Overwriting requires that the media be in working order. *Degaussing* is a method to magnetically erase data from magnetic media.

Two types of degausser exist: strong magnets and electric degaussers. The final method of sanitization is *destruction* of the media such as shredding paper or diskettes.

14.8 Documentation

Documentation of all aspects of computer support and operations is important to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help assure that operations will be performed correctly and efficiently.

The security of a system also needs to be documented. This includes many types of documentation such as security plans, contingency plans, risk analyses, and security policies and procedures. Much of this information, particularly risk and threat analyses, must be protected against unauthorized disclosure. Security documentation also needs to be both current and accessible. The accessibility needs of security documentation should take into account special factors (such as the need to find the contingency plan during a disaster).

Security documentation should be designed to fulfill the needs of the different types of people who use it. For this reason, many organizations separate documentation into *policy* and *procedures*. A *security procedures manual* should be written to inform a given group of system users how to their jobs in a secure manner. A security procedures manual for systems operations and support staff may address a wide variety of technical and operational concerns in considerable detail.

14.9 Maintenance

The maintenance of a system requires either physical or logical access to the system. From a security perspective it is important to ensure that security breaches do not occur through maintenance channels.

Maintenance may be performed by support and operations staff, by hardware or software vendors, or by third party service providers. Maintenance may be performed on site, or it may be necessary to move equipment to a repair site. Maintenance may also be performed remotely via communications connections.

Maintenance involves special access to the system. If the maintenance is performed by someone who does not normally have access to the system, then a security vulnerability is introduced.

In limited circumstances, it may be necessary to take additional precautions such as conducting a background investigation of service provider personnel. Supervision of maintenance personnel may prevent some problems, such as "snooping around" the physical area. However, it is very difficult to prevent damage done through the maintenance process.

One of the most common methods for hackers to break into systems is to use maintenance accounts which still have factory-set or easily guessed passwords.

There have been cases where maintenance personnel unintentionally harmed a system by introducing a virus. Maintenance personnel can intentionally harm a system, such as introducing software that contains a trojan horse. However, supervision of the maintenance personnel will normally not catch these problems.

Many computer systems provide *maintenance accounts*. These special login accounts are normally pre-configured at the factory with pre-set, widely known passwords. *It is critical to change these passwords and otherwise disable the accounts until they are needed.* Procedures should be developed to ensure that only authorized maintenance personnel can use these accounts. If the account is to be used remotely, authentication of the maintenance provider can be performed using call-back confirmation. This helps ensure that remote diagnostic activities actually originate from an established phone number at the vendor's site. Other techniques can also help, including: encryption and decryption of diagnostic communications, strong identification and authentication techniques such as tokens, and remote disconnect verification.

Special considerations for larger systems: These systems may have *diagnostic ports*. In addition, manufacturers of larger systems and third party providers may offer more diagnostic and support services. It is critical to ensure that these ports are only used by authorized personnel and cannot be accessed by hackers.

14.10 Interdependencies

There are support and operations components in all of the operational and technical controls. *Personnel*. Most support and operations staff have special access to the system. Some organizations conduct background checks on individuals filling these positions.

Incident Handling. Support and operations may include an organization's incident handling staff. Even if they are separate organizations, they must work together to recognize and respond to incidents.

Contingency Planning. Support and operations normally provides technical input to contingency planning and carries out the activities of making backups, updating documentation, and practicing response to contingencies.

Security Awareness, Training, and Education. Support and operations staff must be trained in security procedures and aware of the importance of security. In addition, they many provide technical expertise needed to teach users how to secure their systems.

Physical and Environmental. Support and operations staff often control the immediate physical area around the computer system.

Technical controls. The technical controls are installed, maintained, and used by support and operations staff. They create the user accounts, read audit logs, create user profiles and menus, control bulk encryption over telecommunications links, and perform the countless operational tasks needed to use technical controls effectively.

In addition, support and operations also has interdependencies with some of the management controls.

Assurance. Support and operations staff ensure that changes to a system do not introduce security vulnerabilities by using assurance methods to evaluate or test the changes. Operational assurance is normally performed by support and operations staff.

Life Cycle. The ongoing activities performed by support and operations staff is critical to effective life cycle management.

14.11 Cost Considerations

The cost of ensuring adequate security in day-to-day support and operations is largely dependent upon the size and characteristics of the operating environment and the nature of the processing being performed. If sufficient support personnel are already available, it is important that they be trained in the security aspects of their assigned jobs, but it is usually not necessary to hire additional support and operations security specialists. Security training, both initial and ongoing, is a cost of successfully incorporating security measures into support and operations activities.

Another cost consideration is that associated with creating and/or updating documentation to ensure that security concerns are appropriately reflected in support and operations procedures and duties.

14.12 Summary

Support and operations can be an Achilles' heel for many organizations. This is because it is often given relatively little attention compared to what may seem like larger security concerns. Support and operations involves such seemingly ordinary activities not directly tied to threats and emergencies. However, if the most basic, routine system support does not also reflect appropriate security measures, the security of the system may be severely weakened.

14.13 References

Bicknell, Paul. "Data Security for Personal Computers." *Proceedings of the 15th National Computer Security Conference*, Vol. I, 1992.

Caelli, Wm, et al. *Information Security Handbook*. Stockton Press, 1991.

Carnahan, Lisa J. "A Local Area Network Security Architecture." *Proceedings of the 15th National Computer Security Conference*, Vol. I, 1992.

Carroll, J.M. *Managing Risk: A Computer-Aided Strategy*, Butterworths Boston, 1984.

Chapman, D. Brent. "Network (In)Security Through IP Packet Filtering." *Proceedings of the 3rd USENIX UNIX Security Symposium*, 1992.

Curry, David A. *UNIX System Security: A Guide for Users and System Administrators.* Addison-Wesley Publishing Co., Inc.,1992.

Garfinkel, Simson and Gene Spafford. *Practical UNIX Security*. O'Reilly, 1991.

Holbrook, Paul and Joyce Reynolds eds., *Site Security Handbook*, available by anonymous ftp from nic.ddn.mil (in rfc directory).

Internet Security for System & Network Administrators. CERT Security Seminars, CERT Coordination Center, 1993.

Murray, W.H., "Security Considerations for Personal Computers." *Tutorial: Computer and Network Security*. IEEE Computer Society Press, 1986.

Parker, Donna B. *Managers Guide to Computer Security*. Reston Publishing, Inc., 1981.

Peele, Horace. "Defense Against Computer AIDS." *Proceedings of the 15th National Computer Security Conference*, Vol. I, 1992.

Pfleeger, Charles P. *Security in Computing*. Prentice-Hall, Inc., 1989.

Varadhan, Kannan. "OARnet Security Procedures." OARnet Engineering Group, 1992.

15 Physical and Environmental Security

15.1 Introduction[60]

The security of a computer system depends upon the environment in which it operates. Consequently, physical security must be addressed in the overall management of risk to system resources. The term, *physical and environmental security*, as used in this chapter, refers to measures taken to protect systems, buildings and related supporting infrastructure upon which system resources depend against threats associated with the physical environment. Physical and environmental security controls extend to include the following three broad areas:

1) *The Physical Facility* -- usually the building, other structure, or vehicle, housing the system and network components.

> Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used for to support their operation.

Systems can be characterized, based upon their operating location, as static, mobile, or portable. Static systems are located permanently in structures at fixed locations. Mobile systems are installed in vehicles that perform the function of a structure, but not at a fixed location. Portable systems does not have a fixed operating location. They may be operated in wide variety of locations, including buildings or vehicles, or in the open. The characteristics of these structures and vehicles (the physical facility) determine some of the physical threats such as fire, roof leaks, or unauthorized physical access.

2) *The Operating Location* -- the general geographic location of the facility.

The operating location of systems determine the characteristics of additional threats including *natural threats*, which include earthquakes and flooding; *man-made threats* such as burglary, civil disorders, or interception of transmissions and emanations; and *damaging nearby activities*, including toxic chemical spills, explosions, fires, and electromagnetic interference from emitters such as radars.

3) *Supporting Facilities* -- those services (both technical and human) which underpin the operation of the system.

The operation of a system usually depends on supporting facilities such as electric power, heating and air conditioning, and telecommunications. The failure or substandard performance of these facilities may interrupt operation of the systems and may cause physical

[60] This chapter is drawn upon work by Robert V. Jacobson, funded by the Tennessee Valley Authority.

damage to system hardware or stored data.

This chapter first discusses the benefits of physical security measures. Next, the chapter presents an overview of common physical and environmental security controls. A short discussion of cost-effective implementation of controls follows. Interdependencies with other controls and cost considerations are then discussed. Finally, a brief summary and sources of further information are provided.

15.2 Benefits

Physical and environmental security measures protect system resources against many types of losses. Major kinds of losses are described below.

Interruptions in Providing Computer Services. An external threat may cause an interruption to the scheduled operation of a system. This prevents normal operation by end users of the system. The magnitude of the losses depends on the duration and timing of the service interruption and the characteristics of the operations performed by end users.

Physical Damage. If system hardware is damaged or destroyed, it usually must be repaired or replaced. Data may be destroyed as an act of sabotage by a physical attack on data storage media (e.g., rendering it unreadable or only partly readable). If data stored by a system for operational use is destroyed or corrupted, it must be restored from back-up copies or from the original sources before the system can be used. The magnitude of a physical damage loss depends on the cost to repair or replace the damaged hardware *and* data as well as costs arising from service interruptions.

Unauthorized Disclosure of Information. The physical characteristics of the facility housing a system may permit an intruder to gain access to media (including both media external to system hardware -- such as diskettes, tapes and printouts -- and media within system components such as fixed disks), or transmission lines or display screens containing disclosure-sensitive information. This may include stored information such as password lists.

Loss of Control over System Integrity. If an intruder gains access to the central processing unit, it is usually possible to re-boot the system, and *bypass* logical access controls. This can lead to information disclosure, fraud, replacement of system and application software, introduction of a trojan horse, and more. Moreover, if such access is gained, it may be very difficult to determine what has been modified, lost, or corrupted.

Physical Theft. System hardware may be stolen. The magnitude of the loss is determined by the cost to replace the stolen hardware including restoration of data stored on stolen media. A theft may also cause a service interruption.

15.3 Specific Areas of Consideration

This section discusses seven major areas in which physical and environmental security controls are useful. These include:

- Physical access controls,
- Fire safety,
- Supporting utilities,
- Structural collapse,
- Plumbing leaks,
- Interception of data, and
- Mobile and portable systems.

15.3.1 Physical Access Controls

Physical access controls restrict the entry and exit or personnel (and often equipment and media) from an area (such as an office building, suite, data center, or room containing a LAN server).

The controls over physical access to the elements of a system can be thought of as consisting of controlled areas, barriers that isolate each area, entry points in the barriers, and screening measures employed at each of the entry points. In addition, staff members who work in a restricted area serve an important role in providing physical security as they can be trained to challenge persons they do not recognize.

Life Safety

It is important to understand that physical access control objectives may be in conflict with *life safety*. Simply stated, life safety aims at unlocking every door, and access controls strive to lock all doors. In general life safety must be given first consideration, but it is usually possible to find arrangements that meet both goals. For example, it is often possible to equip emergency exit doors with a time delay. When one pushes on the panic bar, a loud alarm sounds, and the door is released after a brief delay. The expectation is that people will be deterred from using such exits improperly, but will not be significantly endangered during an emergency evacuation.

Physical access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, the electric power service, the air conditioning and heating plant, telephone and data lines, back-up media and source documents, and any other elements required for operation of the system. This means all the areas in the building(s) that contain system elements must be identified.

It is also important to review the effectiveness of physical controls to each area, both during normal business hours, and at other times -- particularly when an area may be unoccupied. Effectiveness depends on both the characteristics of the control devices used (e.g., key-card controlled doors) and the effectiveness of the implementation and operation (e.g., the degree to which "tailgating" is tolerated). Statements to the effect that "only authorized persons can enter this area" are not particularly meaningful. It must be determined if intruders can easily defeat the controls, the extent to which strangers are challenged, and the effectiveness of other control procedures. Factors like these modify the effectiveness of physical controls.

There are many types of physical access controls, including: badges, memory cards, guards, keys, true floor to ceiling wall construction, fences, locks, and so forth.

The feasibility of surreptitious entry must also be considered. For example, it may be possible to go over the top of a partition that stops at the underside of a suspended ceiling or cut a hole in a plaster board partition in a location hidden by furniture. If a door is controlled by a combination lock, it may be possible to observe an authorized person entering the lock combination. If key-cards are not carefully controlled, an intruder may be able to steal a card left on a desk or use a card passed back by an accomplice.

Corrective actions can address any of the factors listed above. Adding an additional barrier reduces the level of threat to more restricted interior areas. By enhancing the screening at an entry point the number of penetrations can be reduced. For example, a guard will provide a higher level of screening than a card key controlled door. Reorganizing traffic patterns, work flow, and work areas may make it feasible to reduce the number of persons who must have access to a restricted area. Physical modifications to barriers can reduce the vulnerability to surreptitious entry. Intrusion detectors such as closed circuit television cameras, motion detectors, and other devices can detect intruders in unoccupied spaces. Each measure has a costs to install and operate. For example, adding a locked door requires persons using the door to stop and unlock it. Locks also require physical key management and accounting (and re-keying when keys are lost or stolen). Often these effects will be inconsequential, but care should be taken to give then appropriate consideration. As with other security measures, the objective is to select those that are cost beneficial.

15.3.2 Fire Safety

Building fires are a particularly important security threat because of the potential for complete destruction of both hardware and data, the risk to human life, and the pervasiveness of the damage. Experience shows that smoke, corrosive gases, and high humidity from a localized fire can damage systems throughout an entire building. Consequently, it is important to evaluate the fire safety of buildings that house systems. These are important factors in determining the risks from fire:

Ignition Sources. Fires begin because something supplies enough heat to cause other

materials to begin burning. Typical ignition sources are failures of electric devices and wiring, carelessly discarded cigarettes, improper storage of materials subject to spontaneous combustion, improper operation of heating devices, and, of course, arson.

Fuel Sources. If a fire is to grow, it must have a supply of fuel -- material that will burn to support its growth and an adequate supply of oxygen. Once a fire becomes established, it depends on the combustible materials in the building (referred to as the fire load) to support its further growth. The more fuel per square foot, the more intense the fire will be.

Building Operation. If a building is well maintained and operated so as to minimize the accumulation of fuel (such as maintain the integrity of fire barriers) the fire risk will be minimized.

Building Occupancy. Some occupancies are inherently more dangerous that others. This is because of an above average number of potential ignition sources, for example, manufacturing processes using high temperatures, or an above average fuel load, for example, a chemicals warehouse.

Fire Detection. The more quickly a fire is detected, all other things being equal, the more easily it is extinguished, minimizing damage. However, early detection implies a higher false alarm rate, and false alarms can have significant costs. It is also important to pinpoint the location of the fire accurately.

There are four basic kinds of building construction: (a) light frame, (b) heavy timber, (c) incombustible, and (d) fire resistant. Note that the term *fireproof* is not used because no structure can resist a fire indefinitely. Most houses are light frame, and cannot survive more than about thirty minutes in a fire. Heavy timber means that the basic structural elements have a minimum thickness of four inches. When such structures burn, the char that forms tends to insulate the interior of the timber, and so the structure may survive for an hour or more depending on the details. Incombustible means that the structure members will not burn. This almost always means that the members are steel. Note, however, that steel loses it strength at high temperatures, at which point the structure collapses. Fire resistant means that the structural members are incombustible, and are insulated. Typically, the insulation is either concrete that encases steel members, or is a mineral wool that is sprayed onto the members. Of course, the heavier the insulation, the longer the structure will resist a fire.

Note that a building constructed of reinforced concrete can still be destroyed in a fire if there is sufficient fuel present, and fire fighting is ineffective. The prolonged heat of a fire can cause differential expansion of the concrete which causes *spalling*. Portions of the concrete split off, exposing the reinforcing, and the interior of the concrete to additional spalling. Furthermore as heated floor slabs expand outward, they deform supporting columns. Thus, a reinforced concrete parking garage with open exterior walls and a relatively low fire load has a low fire risk, but a similar archival record storage facility with closed exterior walls and a high fire load has a high fire risk and may be destroyed by a fire even though the basic building material is incombustible.

Fire Extinguishment. A fire will burn until it consumes all of the fuel in the building, or it is extinguished. Fire extinguishment may be automatic as with an automatic sprinkler system or a HALON discharge system, or it may be performed by people using portable extinguishers, water hose lines, or other means. The more rapid and effective the application

of extinguishment, the more quickly a fire will be extinguished. A fire may be extinguished by cooling the fire site with a stream of water, by limiting the supply of oxygen with a blanket of foam or powder, or by breaking the combustion chemical reaction chain with a chemical such as HALON-1301.

Experience has shown that automatic sprinkler systems, when properly installed and maintained and provided with an adequate supply of water, are highly effective in protecting buildings and their contents. Nonetheless, one often hears uninformed persons speak of the *water damage* done by sprinkler systems as a disadvantage. Of course, sprinklers do not cause water damage. *Fires that trigger sprinkler systems* cause the damage.[61] On reflection, one can see that if a sprinkler system were turned off to *prevent water damage*, the damage caused by fires would *increase*, not decrease. In short, sprinkler systems reduce fire damage, protect the lives of building occupants, and limit the fire damage to the building itself. All these factors contribute to more rapid recovery of systems following a fire.

Each of these factors is important to an assessment of the occurrence rate of fires and an estimate of the amount of damage that will result. The objective of a fire safety program is to optimize these factors within the constraints imposed by the use made of the building to minimize the risk of fire.

Halons have been identified as substances which harm the Earth's protective ozone layer. So, under an international agreement (known as the Montreal Protocol), productions of halons ended January 1, 1994. In September 1992, the General Services Administration issued a moratorium on halon use by federal agencies.

15.3.3 Failure of Supporting Utilities

Systems and the people who operate them must have a reasonable operating environment. Consequently, failures of heating and air conditioning system will usually cause a service interruption and might damage hardware. These utilities are composed of many elements, each of which must function properly. For example, the typical air conditioning system consists of (a) air handlers that cool and humidify room air, (b) circulating pumps that send chilled water to the air handlers, (c) chillers that extract heat from the chiller water, and (d) cooling towers that discharge the heat to the outside air. Each of these elements has a mean-time-between-failures (MTBF) and a mean-time-to-repair (MTTR). Using the MTBF and MTTR values for each of the elements of a system, estimates of the occurrence rate of system failures and the range of resulting service interruptions can be made.

This same line of reasoning applies to electric power distribution, heating plants, water, sewage, and other utilities required for system operation or staff comfort. By identifying the failure modes of each utility and estimating the MTBF and MTTR, the necessary failure

[61] Occurrences of accidental discharge are extremely rare, and, in a fire, only the sprinkler heads in the immediate area of the fire open and discharge water.

threat parameters can be developed to calculate the resulting risk. The risk of utilities failure can be reduced in several ways. Units with lower MTBF values can be substituted. MTTR can be reduced by stocking spare parts on site and training maintenance personnel. The outages resulting from a given MTBF can be reduced by installing redundant units under the assumption that failures are distributed randomly in time. Each of these strategies is evaluated by comparing the reduction in risk with the cost to achieve it.

15.3.4 Structural Collapse

It is possible that a building may be subjected to a load greater than it can support. Most commonly this is a result of an earthquake, a snow load on the roof beyond design criteria, an explosion that displaces or cuts structural members, or a fire that weakens structural members. Even if the structure is not completely demolished, the authorities may decide to ban its further use, sometimes even banning entry to remove materials. This threat applies primarily to high rise buildings and those with large interior spaces without supporting columns.

15.3.5 Plumbing Leaks

While plumbing leaks do not occur everyday, they can be seriously disruptive. By consulting the building's plumbing drawings, the location of plumbing lines that might endanger system hardware can be identified. These lines include hot and cold water, chilled water supply and return lines, steam lines, automatic sprinkler lines, fire hose standpipes, and drains. If a building includes a laboratory or manufacturing spaces, there may be other lines that conduct water, corrosive or toxic chemicals, or gases.

As a rule, analysis often shows that the cost to relocate threatening lines is difficult to justify. However, the location of shut-off valves and procedures that should be followed in the event of a failure must be identified. Operating and security personnel should have this information immediately available for use in an emergency. In some cases it may be possible to relocate system hardware, particularly distributed LAN hardware.

15.3.6 Interception of Data

Depending on the type of data processed by a system there may be a significant exposure to interception of the data. This may take a number of forms such as these:

Direct Observation. System terminals and workstations may be located such that their display screens can be observed by unauthorized persons. In most cases it is relatively easy to relocate the display to eliminate the exposure.

Interception of Data Transmissions. If an intruder can gain access to data transmission lines, it may be feasible to tap into the lines and read the data being transmitted. Of course, the intruder cannot control what is transmitted, and so may not be able to immediately observe data of interest. However, over a period of time there may be a serious level of disclosure.

Local area networks typically broadcast messages. Consequently, all traffic, including passwords, could be retrieved. Intruders could also transmit spurious data on tapped lines -- either for purposes of disruption or fraud.

Electromagnetic Interception. Systems routinely radiate electromagnetic energy that can be detected with special purpose radio receivers. Successful interception will depend on the signal strength at the receiver location; the greater the separation between the system and the receiver, the lower the success rate. The signal to noise ratio at the receiver, determined in part by the number of competing emitters will also affect the success rate. The more workstations of the same type in a given location, the more difficult it is to intercept a given workstation's radiation. On the other hand, the trend toward wireless (i.e., deliberate radiation) LAN connections may increase the likelihood of successful interception.

15.3.7 Mobile and Portable Systems

The analysis and management of risk must be modified if a system is installed in a vehicle or is portable such as a laptop computer. The system in a vehicle will share the risks of the vehicle including accidents and theft as well as regional and local risks. There may be periods when the system is left unattended, increasing the risk of unauthorized access and theft.

Portable and mobile systems share an increased risk of theft and physical damage. In addition, portable systems can be "misplaced" by careless users. Laptop computers are sometimes required to be stored securely when not in use.

Encryption of data files on stored media may also prove a cost-effective precaution against disclosure of confidential information if a laptop computer is lost or stolen.

If a mobile or portable system uses particular valuable or important data, it may be appropriate to store its data on a medium that can be removed from the system when it is unattended or to encrypt the data. In any case, the issue of how custody of mobile and portable computers are to be controlled must be addressed. Depending on the sensitivity of the system and its application, it may be appropriate to require briefings of users with signed briefing acknowledgments. (See the Personnel/User chapter for an example.)

15.4 Approach to Implementation

This section discusses the various ways that cost-effective controls are selected.

Physical and environmental security controls, like other security measures, are selected because they are cost-beneficial. This does not mean that a user must conduct a detailed cost benefit analysis for the selection of every control. There are four general ways to justify the selection of controls:

It is required by law or regulation. Fire exit doors with panic bar hardware and exit lights are examples of such security measures. Presumably, the regulatory authority has considered the cost-benefit and has determined that it is in the interest of the public to require that the security measure be implemented. A lawfully conducted organization has no option and must implement all such required security measures.

The cost is insignificant but the benefit is material. A good example is a facility with a low-traffic door to a restricted access area equipped with a key-lock. The cost of keeping the door locked is minimal but there is a significant benefit. Once a significant benefit/minimal cost security measure has been identified, no further analysis is required to justify implementation of the security measure.

The security measure addresses a potentially "fatal" security exposure but has a reasonable cost. Backing up system software and data is an example. For most systems, the cost to make regular back-up copies is modest (compared to the costs of operating the system), the organization would not be able to function if the stored data were lost, and the cost impact of the failure would be material. In such cases, it would not be necessary to develop any further cost-justification for the back-up of the software and data. However, this justification depends on what constitutes a *modest* cost, and it does not identify the optimum back-up schedule. Broadly speaking, a cost that does not require budgeting of additional funds would qualify.

The security measure is estimated to be cost-beneficial. In this context, *cost-beneficial* means that the reduction in expected loss is significantly greater than the cost to implement the security measure. In other words, the cost of the security measure is justified by the reduction in expected loss that it is expected to yield.

The last reason, estimated cost-beneficial security measures, is the most complex of the four and requires a more detailed analysis. Simple rules-of-thumb do not apply. Consider, for example, the threat of electric power failure and the security measures that can protect against their harm. The threat parameters, rate of occurrence and range of outage durations depend on the location of the system, the details of its connection to the local electric power utility, the details of the internal power distribution system, and the character of other activities in the building that use electric power. The service interruption loss potential of the system depends on the details of the functions it performs. Two systems that are otherwise identical can support functions that have quite different degrees of urgency. Thus, two systems may have the same electric power failure threat and vulnerability parameters, but entirely different loss potential parameters.

Furthermore, there are a number of different security measures available to address electric power failures. These measures differ in both cost and performance. For example, the cost of an uninterruptible power supply (UPS) depends on the size of the electric load it can support, the number of minutes it can support the load, and the speed with which it assumes the load when the primary power source fails. An on-site power generator could also be

installed either in place of a UPS (accepting the fact that a power failure will cause a brief service interruption) or in order to provide long term back-up to a UPS system. Design decisions include the magnitude of the load the generator will support, the size of the on-site fuel supply, and the details of the facilities to switch the load from the primary source or the UPS to the on-site generator.

This example shows systems with a wide range of risks and a wide range of available security measures (including, of course, no action), each with its own cost factors and performance parameters. If the cost of a potential security measure is significant, and it cannot be justified by any of the first three reasons listed above, then its cost (both implementation and on-going operation) and its benefit (reduction in future expected losses) must be analyzed to determine if it is cost-beneficial. The electric power example shows that many factors affect the analysis. This is why one cannot depend on simple rules of thumb to make prudent decisions.

15.5 Interdependencies

Physical and environmental security measures rely on and support the proper functioning of many of the other areas discussed in this Handbook. Among the most important are:

Logical Access Controls - Physical security controls augment logical access controls. Even if the most advanced and well implemented logical access controls are in place, but inadequate physical security measures are implemented, logical access controls may be circumvented by directly accessing the hardware and storage media.

Risk Management - Physical and environmental controls can be expensive (and sometimes user-unfriendly). Their selection should always be based upon a sound risk management approach, as discussed earlier.

Contingency Planning - A large portion of the contingency planning process involves the failure of physical and environmental controls. Having sound controls, therefore, can help minimize losses from such contingencies.

Identification and Authentication (I&A) - Many physical access control systems require that people be identified and authenticated. Automated physical security access controls can use the same types of I&A as other computer systems. In addition, it is possible to use the same tokens (e.g., badges) as those used for other computer-based I&A.

Other - Physical and environmental controls are also closely linked to the activities of the local guard force, fire house, life safety office, and medical office. These organizations should be consulted for their expertise in planning controls for the systems environment.

15.6 Cost Considerations

Costs associated with physical security measures range greatly. Some measures, such as keeping a door locked, may be trivially inexpensive. Other systems, such as the installation of fire detection and suppression systems can be far more costly. Useful generalizations about costs, therefore, are difficult make.

15.7 Summary

Physical security controls play an important role in the protection of system resources. They augment logical access controls in protecting data against unauthorized modification, protect the availability of system resources, and guard against unauthorized disclosure of information.

15.8 References

Alexander, M. (editor) "Secure Your Computers and Lock Your Doors" *Infosecurity News*. 4(6), 1993. pp. 80-85.

Archer, R. "Testing: Following Strict Criteria" *Security Dealer*. 15(5), 1993. pp. 32-35.

Chanaud, R. "Keeping Conversations Confidential." *Security Management*. 37(3), 1993. pp. 43-48.

Guidelines for ADP Physical Security and Risk Management. FIPS PUB 31. National Institute of Standards and Technology, June 1974.

Miehl, F. "The Ins and Outs of Door Locks." *Security Management*. 37(2), 1993. pp. 48-53.

Peterson, P. "Infosecurity and Shrinking Media." *ISSA Access*. 5(2), 1992. pp. 19-22.

Roenne, G. "Devising a Strategy Keyed to Locks." *Security Management*. 38(4), 1994. pp. 55-56.

Zimmerman, J. "Using Smart Cards - A Smart Move." *Security Management*. 36(1), 1992. pp. 32-36.