Chapter 10

PERSONNEL/USER ISSUES

Many important issues in computer security involve human users, designers, implementors, and managers. A broad range of security issues relate to how these individuals interact with computers and the access and authorities they need to do their job. No computer system can be secured without properly addressing these security issues.[77]

This chapter examines issues concerning the staffing of positions that interact with computer systems; the administration of users on a system, including considerations for terminating employee access; and special considerations that may arise when contractors or the public have access to systems. Personnel issues are closely linked to logical access controls, discussed in Chapter 17.

10.1 Staffing

The staffing process generally involves at least four steps and can apply equally to general users as well as to application managers, system management personnel, and security personnel. These four steps are: (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 and selecting an individual; and (4) training.

10.1.1 Groundbreaking – Position Definition

Early in the process of defining a position, security issues should be identified and dealt with. Once a position has been broadly defined, the responsible supervisor should determine the type of computer access needed for the position. There are two general principles to apply when granting access: *separation of duties* and *least privilege*.

Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. For example, in financial systems, no single individual should normally be 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 need to be designed into both the process as well as the specific, individual positions of personnel who will implement the process. Ensuring that such duties are well defined is the responsibility of management.

Least privilege refers to the security objective of granting users *only those accesses they need to*

[77] 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).

perform their official duties. Data entry clerks, for example, may not have any need to run analysis reports of their database. However, least privilege does not mean that all users will have extremely little functional access; some employees will have significant access if it is required for their position. However, applying this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources. It is important to make certain that the implementation of least privilege does not interfere with the ability to have personnel substitute for each other without undue delay. Without careful planning, access control can interfere with contingency plans.

10.1.2 Determining Position Sensitivity

Knowledge of the duties and access levels that a particular position will require is necessary for determining the sensitivity of the position. The responsible management official should correctly identify position sensitivity levels so that appropriate, cost-effective screening can be completed.

Various levels of sensitivity are assigned to positions in the federal government. Determining the appropriate level is based upon such factors as the type and degree of harm (e.g., disclosure of private information, interruption of critical processing, computer fraud) the individual can cause through misuse of the computer system as well as more traditional factors, such as access to classified information and fiduciary responsibilities. Specific agency guidance should be followed on this matter.

It is important to select the appropriate position sensitivity, since controls in excess of the sensitivity of the position wastes resources, while too little may cause unacceptable risks.

10.1.3 Filling the Position -- Screening and Selecting

Once a position's sensitivity has been determined, the position is ready to be staffed. In the federal government, this typically includes publishing a formal vacancy announcement and identifying which applicants meet the position requirements. More sensitive positions typically require *preemployment* background screening; screening after employment has commenced (post-entry-on-duty) may suffice for less sensitive positions.

> In general, it is more effective to use separation of duties and least privilege to limit the sensitivity of the position, rather than relying on screening to reduce the risk to the organization.

Background screening helps determine whether a particular individual is suitable for a given position. For example, in positions with high-level fiduciary responsibility, the screening process will attempt to ascertain the person's trustworthiness and appropriateness for 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).

Within the Federal Government, the most basic screening technique involves a check for a criminal history, checking FBI fingerprint records, and other federal indices.[78] More extensive background checks examine other factors, such as a person's work and educational history, personal interview, history of 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 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 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 compromising in a person's background does not necessarily mean they are unsuitable for a particular job. A determination should 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*.

10.1.4 Employee Training and Awareness

Even after a candidate has been hired, the staffing process cannot yet be considered complete **–** employees still have to be trained to do their job, which includes computer security responsibilities and duties. As discussed in Chapter 13, 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 they are granted any access to computer systems. Others argue that this must be a risk-based decision, perhaps granting only restricted access (or, perhaps, only access to their PC) until the required training is completed. Both approaches recognize that adequately trained employees are crucial to the effective functioning of computer systems and applications. Organizations may provide introductory training prior to granting any access with follow-up more extensive training. In addition, although training of new users is critical, it is important to recognize that security training and awareness activities should be ongoing during the time an

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

individual is a system user. (See Chapter 13 for a more thorough discussion.)

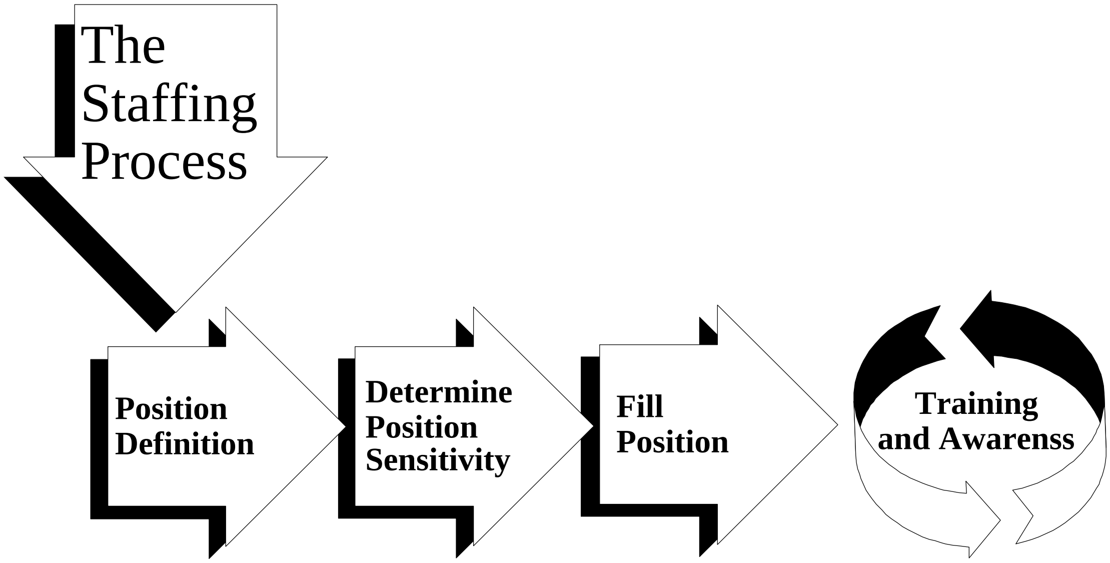

Figure 10.1

10.2 User Administration

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

10.2.1 User Account Management

User account management involves (1) the process of requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing 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 ensure 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 authorizations. 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 authorizations 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., user ID) and a means of authentication (e.g., password or smart card/PIN). One issue that may arise at this stage is whether the user ID 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). Tying user IDs to positions may simplify administrative overhead in some cases; however, it may make auditing more difficult as one tries to trace the actions of a particular individual. It is normally more advantageous to tie the user ID to the individual employee. However, if the user ID is created and tied to a position, procedures will have to be established to change them if employees switch jobs or are otherwise reassigned.

When 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 an "acknowledgment statement," which may also state causes for dismissal or prosecution under the Computer Fraud and Abuse Act and other applicable state and local laws.[79]

When user accounts are no longer required, the supervisor should inform the application manager and system management office so 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 of this chapter.

Sample User Account and Password Acknowledgment Form

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 system 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 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.

It is essential to realize that *access and authorization administration is a continuing process*. New user accounts are added while others 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 to allow users access to only 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 granted the authority to create accounts and change user access authorizations or to 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.

10.2.2 Audit and Management Reviews

From time to time, it is necessary to review user account management on a system. Within the area of user access issues, such reviews may examine the levels of access each individual has, conformity 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.

[79] Whenever users are asked to sign a document, appropriate review by organizational legal counsel and, if applicable, by employee bargaining units should be accomplished.

These reviews can be conducted on *at least* two levels:[80] (1) on an application-by-application basis or (2) on a systemwide basis. Both kinds of reviews can be conducted by, among others, in-house systems personnel (a self-audit), the organization's internal audit staff, or external auditors. For example, a good practice is for application managers (and data owners, if different) to review all access levels of all application users every month – and sign a formal access approval list, which will provide a written record of the approvals. While it may initially 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 that their managers have specified. However because access requirements may change over time, it is important to involve the application manager, who is often the only individual in a position to know current access requirements.

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 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 examine non-computer access by reviewing, for example, who should have physical access to the check printer or blank-check stock.)

10.2.3 Detecting Unauthorized/Illegal Activities

Several mechanisms are used besides auditing[81] and analysis of audit trails to detect unauthorized and illegal acts. (See Chapters 9 and 18.) 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, for example, if problems are saved for the employees 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 periods of absence. Particularly within the government, periodic rescreening of personnel is used to identify possible indications of illegal activity (e.g., living a lifestyle in excess of known income level).

10.2.4 Temporary Assignments and In-house Transfers

One significant aspect of managing a system involves keeping user access authorizations up to date. Access authorizations 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

[80] Note that this is not an either/or distinction.

[81] The term *auditing* is used here in a broad sense to refer to the review and analysis of past events.

(e.g., after an in-house transfer) and (2) termination discussed in the following section.

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

Permanent changes are usually necessary when employees change positions within an organization. In this case, the process of granting account authorizations (described in Section 10.2.1) will occur again. At this time, however, is it also important that access authorizations of the prior position be removed. Many instances of "authorization creep" have occurred with employees continuing to maintain access rights for previously held positions within an organization. This practice is inconsistent with the principle of least privilege.

10.2.5 Termination

Termination of a 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,"[82] or involuntarily transferred. Fortunately, the former situation is more common, but security issues have to be addressed in both situations.

10.2.5.1 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. Out-processing often involves a sign-out form initialed by each functional manager with an interest in the separation. This normally includes the group(s) managing access controls, the control of keys, the briefing on the responsibilities for confidentiality and privacy, the library, the property clerk, and several other functions not necessarily related to information security.

In addition, other issues should be examined as well. The continued availability of data, for example, must often be assured. In both the manual and the electronic worlds, this may involve documenting procedures or filing schemes, such as how documents are stored on the hard disk, and how are they backed up. Employees should be instructed whether or not to "clean up" their

[82] *RIF* is a term used within the government as shorthand for "reduction in force."

PC before leaving. If cryptography is used to protect data, the availability of cryptographic keys to management personnel must be ensured. Authentication tokens must be collected.

Confidentiality of data can also be an issue. 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 organizational-specific issues should be addressed throughout an organization to ensure continued access to data and to provide continued confidentiality and integrity during personnel transitions. (Many of these issues should be addressed on an ongoing basis, not just during personnel transitions.) The training and awareness program normally should address such issues.

10.2.5.2 Unfriendly Termination

Unfriendly termination involves the removal of an employee under involuntary or adverse conditions. This may include termination for cause, RIF, involuntary transfer, resignation for "personality conflicts," and situations with pending grievances. The tension in such terminations may multiply and complicate security issues. Additionally, all of the issues involved in friendly terminations are still present, but addressing them may be considerably more difficult.

The greatest threat from unfriendly terminations is likely to come from those personnel who are capable of changing code or modifying 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 that 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, and other "random" errors can be made. Correcting these situations can be extremely 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 employees are to be fired, system access should be removed at the same time (or just before) the employees are notified of their dismissal. When an employee notifies an organization 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 employees capable of changing programs or modifying the system or applications. In other cases, physical removal from their offices (and, of course, logical removal, *when logical access controls exist*) may suffice.

10.3 Contractor Access Considerations

Many federal agencies as well as private organizations use contractors and consultants to assist with computer processing. Contractors are often used for shorter periods of time than regular employees. This factor may change the cost-effectiveness of conducting screening. The often higher turnover among contractor personnel generates additional costs for security programs in terms of user administration.

10.4 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 to 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 on the confidentiality, availability, and integrity of information processed by a system. 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.

OMB Circular A-130, Appendix III "Security of Federal Automated Information" and NIST *CSL Bulletin* "Security Issues in Public Access Systems" both recommend segregating information made directly accessible to the public from official records.

Besides increased risk of hackers, public access systems can 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 in order to embarrass or discredit the organization. Attacks on public access systems could have a substantial impact on the organization's reputation and the level of public confidence due to the high 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 that often involve some user training and frequently require the signing of forms acknowledging user responsibilities. In addition, user profiles can be created and sophisticated audit mechanisms can be 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 may be tolerated. However, when opening up a system to public access, additional precautions may be necessary because of the increased threats.

10.5 Interdependencies

User issues are tied to topics throughout this handbook.

Training and Awareness discussed in Chapter 13 is a critical part of addressing the user issues of computer security.

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 do, points to the importance of considering user issues in the computer security picture, and the importance of *Auditing*.

Policy, particularly its compliance component, is closely linked to personnel issues. A deterrent effect arises among users when they are aware that their misconduct, intentional or unintentional, will be detected.

These controls also depend on manager's (1) selecting the right type and level of access for their employees and (2) informing system managers of which employees need accounts and what type and level of access they require, and (3) promptly informing system managers of changes to access requirements. Otherwise, accounts and accesses can be granted to or maintained for people who should not have them.

10.6 Cost Considerations

There are many security costs under the category of user issues. Among these are:

Screening -- Costs of initial background screening and periodic updates, as appropriate.[83]

Training and Awareness -- Costs of training needs assessments, training materials, course fees, and so forth, as discussed separately in Chapter 13.

User Administration -- Costs of managing identification and authentication which, particularly for

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

large distributed systems, may be rather significant.

Access Administration -- Particularly beyond the initial account set-up, are ongoing costs of maintaining user accesses currently and completely.

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

References

Fites, P., and M. Kratz. *Information Systems Security: A Practitioner's Reference*. New York, NY: Van Nostrand Reinhold, 1993. (See especially Chapter 6.)

National Institute of Standards and Technology. "Security Issues in Public Access Systems." Computer Systems Laboratory Bulletin. May 1993.

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.

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.

Chapter 11

PREPARING FOR CONTINGENCIES AND DISASTERS

A *computer security contingency* is an event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions. Such an event could be a power outage, hardware failure, fire, or storm. If the event is very destructive, it is often called a disaster.[84]

To avert potential contingencies and disasters or minimize the damage they cause organizations can take steps early to control the event. Generally called *contingency planning*,[85] this activity is closely related to incident handling, which primarily addresses malicious technical threats such as hackers and viruses.[86]

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

Contingency planning involves more than planning for a move offsite after a disaster destroys a data center. It also addresses how to keep an organization's 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 presents the contingency planning process in six steps:[87]

1. *Identifying the mission- or business-critical functions*.

2. *Identifying the resources that support the critical functions.*

3. *Anticipating potential contingencies or disasters*.

4. *Selecting contingency planning strategies*.

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

[85] Other names include disaster recovery, business continuity, continuity of operations, or business resumption planning.

[86] Some organizations include incident handling as a subset of contingency planning. The relationship is further discussed in Chapter 12, Incident Handling.

[87] 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 functions are addressed.

5. *Implementing the contingency strategies*.

6. *Testing and revising the strategy*.

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

Protecting the continuity of an organization's mission or business is very difficult if it is not clearly identified. Managers need to understand the organization from a point of view that usually extends beyond the area they control. 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 conducting a business, such as manufacturing widgets.

Since the development of a business plan will be used to support contingency planning, it is necessary not only to identify critical missions and businesses, but also to *set priorities for* 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 appropriate priorities have been set (and approved by senior management), it could mean the difference in the organization's ability to survive a disaster.

11.2 Step 2: Identifying the Resources That Support Critical Functions

After identifying critical missions and business functions, it is necessary to identify the supporting resources, the time frames in which each resource is used (e.g., is the resource needed constantly or only at the end of the month?), and the effect on the mission or business of the unavailability of the resource. In identifying resources, a traditional problem has been that different managers oversee different resources. They may not realize how resources interact to support 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, regardless whether they directly relate to a computer.[88]

In many cases, the longer an organization is without a resource, the more critical the situation becomes. For example, the longer a garbage collection strike lasts, the more critical the situation becomes.

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

The analysis of needed resources should be conducted by those who understand how the function is performed and the dependencies of various resources on other resources and other critical relationships. This will allow an organization to *assign priorities* to resources since not all elements of all resources are crucial to the critical functions.

11.2.1 Human Resources

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

Resources That Support Critical Functions

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

11.2.2 Processing Capability

Traditionally contingency planning has focused on processing power (i.e., if the data center is down, how can applications dependent on it continue to be processed?). Although the need for data center backup remains vital, today's other processing alternatives are also important. Local area networks (LANs), minicomputers, workstations, and personal computers in all forms of centralized and distributed processing may be performing critical tasks.

11.2.3 Automated Applications and Data

Computer systems run applications that process data. Without current electronic versions of both applications and data, computerized processing may not be possible. If the processing is being performed on alternate hardware, the applications must be compatible with the alternate hardware, operating systems and other software (including version and configuration), and

Contingency Planning Teams

To understand what resources are needed from each of the six resource categories and to understand how the resources support critical functions, it is often necessary to establish a contingency planning team. A typical team contains representatives from various organizational elements, and is often headed by a contingency planning coordinator. It has representatives from the following three groups:

1. business-oriented groups , 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, and public affairs.

numerous other technical factors. Because of the complexity, it is normally necessary to periodically verify compatibility. (See Step 6, Testing and Revising.)

11.2.4 Computer-Based Services

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

11.2.5 Physical Infrastructure

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 many other items. In addition, computers also need space and utilities, such as electricity. Electronic and paper media used to store applications and data also have physical requirements.

11.2.6 Documents and Papers

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

11.3 Step 3: Anticipating Potential Contingencies or Disasters

Although it is impossible to think of *all* the things that can go wrong, the next step is to identify a likely range of problems. The development of scenarios will help an organization develop a plan to address the wide range of things that can go wrong.

Scenarios should include small and large contingencies. While some general classes of contingency scenarios are obvious, imagination and creativity, as well as research, can point to other possible, but less obvious, contingencies. 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 may 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

1. 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.

2. After the World Trade Center explosion when people reentered the building, they turned on their computer systems to check for problems. Dust and smoke damaged many systems when they 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? Do they have equipment to do their jobs? Can they occupy the building?

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

11.4 Step 4: Selecting Contingency Planning Strategies

The next step is to plan how 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 contingencies, it is necessary to coordinate prevention and recovery efforts.

A contingency planning strategy normally consists of three parts: emergency response, recovery, and resumption.[89] *Emergency response* encompasses the initial actions taken to protect lives and limit damage. *Recovery* refers to the steps that are taken to continue support for critical functions. *Resumption* is the return to normal operations. The relationship between recovery and resumption is important. The longer it takes to resume normal operations, the longer the

[89] Some organizations divide a contingency strategy into emergency response, backup operations, and recovery. The different terminology can be confusing (especially the use of conflicting definitions of *recovery*), although the basic functions performed are the same.

organization will have to operate in the recovery mode.

Example 1: If 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 beforehand 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 on-line information service provided by a commercial vendor. The organization is no longer able to obtain the information manually (e.g., from a reference book) 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, has a contract with the telecommunications carrier to reroute communications to the hot site, has plans to move people, and stores up-to-date copies of data, applications and needed paper 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 two major sites, each of which includes small to medium processors (personal computers and minicomputers). If one site is lost, the other can carry the critical load until more equipment is purchased. Routing of data and voice communications can be performed transparently to redirect traffic. Backup copies are stored at the other site. This plan requires tight control over the architectures used and types of applications that are developed to ensure compatibility. In addition, personnel at both sites must be cross-trained to perform all functions.

The selection of a strategy needs to 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 focus on areas where it is not clear which strategy is the best.

In developing contingency planning strategies, there are many factors to consider in addressing each of the resources that support critical functions. Some examples are presented in the sidebars.

11.4.1 Human Resources

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. The use of additional personnel may introduce security vulnerabilities.

Contingency planning, especially for emergency response, normally places the highest emphasis on the protection of human life.

11.4.2 Processing Capability

Strategies for processing capability are normally grouped into five categories: hot site; cold site; redundancy; reciprocal agreements; and hybrids. These terms originated with recovery strategies for data centers but can be applied to other platforms.

1. *Hot site* – A building already equipped with processing capability and other services.

2. *Cold site* – A building for housing processors that can be easily adapted for use.

3. *Redundant site* – A site equipped and configured exactly like the primary site. (Some organizations plan on having reduced processing capability after a disaster and use partial redundancy. The stocking of spare personal computers or LAN servers also provides some redundancy.)

4. *Reciprocal agreement* – An agreement that allows two organizations to back each other up. (While this approach often sounds desirable, contingency planning experts note that this alternative has the greatest chance of failure due to problems keeping agreements and plans up-to-date as systems and personnel change.)

5. *Hybrids* – Any combinations of the above such as using having a hot site as a backup in case a redundant or reciprocal agreement site is damaged by a separate contingency.

Recovery may include several stages, perhaps marked by increasing availability of processing capability. Resumption planning may include contracts or the ability to place contracts to replace equipment.

11.4.3 Automated Applications and Data

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

The need for computer security does not go away when an organization is processing in a contingency mode. In some cases, the need 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.

11.4.4 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. Hot sites are usually capable of receiving data and voice communications. If one service provider is down, it may be possible to use another. However, the type of communications carrier lost, either local or long distance, is important. Local voice service may be carried on cellular. Local data communications, especially for large volumes, is normally more difficult. In addition, resuming normal operations may require another rerouting of communications services.

11.4.5 Physical Infrastructure

Hot sites and cold sites 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 offsite, procedures need to be developed to ensure a smooth transition back to the primary operating facility or to a new facility. Protection of the physical infrastructure is normally an important part of the emergency response plan, such as use of fire extinguishers or protecting equipment from water damage.

11.4.6 Documents and Papers

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

11.5 Step 5: Implementing the Contingency Strategies

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

11.5.1 Implementation

Much preparation is needed to implement the strategies for protecting critical functions and their supporting resources. For example, one common preparation is to establish procedures for backing up files and applications. Another is to establish contracts and agreements, *if* the contingency strategy calls for them. Existing service contracts may need to be renegotiated to add contingency services. Another preparation may be to purchase equipment, especially to support a redundant capability.

It is important to keep preparations, including documentation, up-to-date. Computer systems change rapidly and so should backup services and redundant equipment. Contracts and agreements may also need to reflect the changes. 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.

Preparation should also include formally designating people who are responsible for various tasks in the event of a contingency. These people are often referred to as the contingency response team. This team is often composed of people who were a part of the contingency planning team.

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. The answers should be documented in organization policy and procedures.

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.

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.

> **Relationship Between Contingency Plans and Computer Security Plans**
>
> For small or less complex systems, the contingency plan may be a part of the computer security plan. For larger or more complex systems, the computer security plan could contain a brief synopsis of the contingency plan, which would be a separate document.

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

11.5.2 Documenting

The contingency plan needs to be written, kept up-to-date as the system and other factors change, and stored in a safe place. A written plan is critical during a contingency, especially if the person who developed the plan is unavailable. It should clearly state in simple language the sequence of tasks to be performed in the event of a contingency so that someone with minimal knowledge could immediately begin to execute the plan. It is generally helpful to store up-to-date copies of the contingency plan in several locations, including any off-site locations, such as alternate processing sites or backup data storage facilities.

11.5.3 Training

All personnel should be trained in their contingency-related duties. New personnel should 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 emergencies. 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 or may not be time to protect equipment and other assets. Practice is necessary in order to react correctly, especially when human safety is involved.

11.6 Step 6: Testing and Revising

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

> Contingency plan maintenance can be incorporated into procedures for change management so that upgrades to hardware and software are reflected in the plan.

A *review* can be a simple test to check the accuracy of contingency plan documentation. For instance, a reviewer could check if individuals listed are still in the organization and still have the responsibilities that caused them to be included in the plan. This test can check home and work telephone numbers, organizational codes, and building and room numbers. The review can determine if files can be restored from backup tapes or if employees know emergency procedures.

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(s) may mentally follow the strategies in the contingency plan, looking for flaws in the logic or process used by the plan's developers. The analyst may also interview functional managers, resource managers, and their staff to uncover missing or unworkable pieces of the plan.

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, flaws in the plan may remain hidden and uncorrected.

Organizations may also arrange *disaster simulations*. These tests provide valuable information about flaws in the contingency plan and provide practice for a real emergency. While they can be expensive, these tests can also provide critical information that can be used to ensure the continuity of important functions. In general, the more critical the functions and the resources addressed in the contingency plan, the more cost-beneficial it is to perform a disaster simulation.

11.7 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 files.

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

11.8 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 provides many benefits and should be performed, although some of the less expensive methods (such as a review) may be sufficient for less critical resources.

References

Alexander, M. ed. "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.

Dykman, C., and C. Davis, eds. *Control Objectives - Controls in an Information Systems Environment: Objectives, Guidelines, and Audit Procedures*, fourth edition. Carol Stream, IL: The EDP Auditors Foundation, Inc., 1992 (especially Chapter 3.5).

Fites, P., and M. Kratz, *Information Systems Security: A Practitioner's Reference*. New York, NY: Van Nostrand Reinhold, 1993 (esp. Chapter 4, pp. 95-112).

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

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

Isaac, I. *Guide on Selecting ADP Backup Process Alternatives*. Special Publication 500-124. Gaithersburg, MD: National Bureau of Standards, November 1985.

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.

Lainhart, J., and M. Donahue. *Computerized Information Systems (CIS) Audit Manual: A Guideline to CIS Auditing in Governmental Organizations*. Carol Stream, IL: The EDP Auditors Foundation Inc., 1992.

National Bureau of Standards. *Guidelines for ADP Contingency Planning*. Federal Information Processing Standard 87. 1981.

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

Chapter 12

COMPUTER SECURITY INCIDENT HANDLING

Computer systems are subject to a wide range of mishaps – from corrupted data files, to viruses, to natural disasters. Some of these mishaps can be 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). More severe mishaps, such as outages caused by natural disasters, are normally addressed in an organization's contingency plan. Other damaging events result from *deliberate malicious technical activity* (e.g., the creation of viruses or system hacking).

A computer security incident can result from a computer virus, other malicious code, or a system intruder, either an insider or an outsider. It is used in this chapter to broadly refer to those incidents resulting from deliberate malicious technical activity.[90] It can more generally refer to those incidents that, without technically expert response, could result in severe damage.[91] This definition of a computer security incident is somewhat flexible and may vary by organization and computing environment.

Malicious code include viruses as well as Trojan horses and worms. A virus is a code segment that replicates by attaching copies of itself to existing executables. A Trojan horse is a program that performs a desired task, but also includes unexpected functions. A worm is a self-replicating program.

Although the threats that hackers and malicious code pose to systems and networks are well known, 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 incidents can often "spread" when left unchecked thus increasing damage and seriously harming an organization.

Incident handling is closely related to contingency planning as well as support and operations. An incident handling capability may be viewed as a component of contingency planning, because it provides the ability to react quickly and efficiently to disruptions in normal processing. Broadly speaking, contingency planning addresses events with the potential to interrupt system operations. Incident handling can be considered that portion of contingency planning that responds to

[90] Organizations may wish to expand this to include, for example, incidents of theft.

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

malicious technical threats.

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*.[92]

Many organizations handle incidents as part of their user support capability (discussed in Chapter 14) or as a part of general system support.

12.1 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.

12.1.1 Containing and Repairing Damage From Incidents

When left unchecked, malicious software can significantly harm an organization's computing, depending on the technology and its connectivity. An incident handling capability provides a way for users to report incidents[93] and the appropriate response and assistance to be provided to aid in recovery. Technical capabilities (e.g., trained personnel and virus identification software) are prepositioned, ready to be used as necessary. Moreover, the organization will have already made important contacts with other supportive sources (e.g., legal, technical, and managerial) to aid in containment and recovery efforts.

> 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 it 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 reinfected. 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.

Without an incident handling capability, certain responses – although well intentioned – can actually make matters worse. In some cases, individuals have unknowingly infected anti-virus software with viruses and then spread them to

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

[93] 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.

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.

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). 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 can require information from outside the organization. By planning ahead, such contacts can be preestablished and the speed of response improved, thereby containing and minimizing damage. Other organizations may have already dealt with similar situations and may have very useful guidance to offer in speeding recovery and minimizing damage.

12.1.2 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 so more effective safeguards can be implemented. 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. The data can be analyzed for patterns – for example, which viruses 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 identifying security solutions. This information will also prove useful in creating a more effective training and awareness program, and thus help reduce the potential for losses. The incident handling capability assists the training and awareness program by providing information to users as to (1) measures that can help avoid incidents (e.g., virus scanning) and (2) what should be done in case an incident does occur.

> The sharing of incident data among organizations can help at both the national and the international levels to prevent and respond to breaches of security in a timely, coordinated manner.

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

12.1.3 Side Benefits

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

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.[94]

Enhancing Internal Communications and Organization Preparedness. Organizations often find that an incident handling capability enhances internal communications and the readiness of the organization to respond to any type of incident, not just computer security incidents. 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 preestablished. The structure set up for reporting incidents can also be used for other purposes.

Enhancing the Training and Awareness Program. The organization's training process can also benefit from incident handling experiences. Based on incidents reported, training personnel will have a better understanding of users' knowledge of security issues. Trainers can use actual incidents 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.

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