Chapter 4

Information Security Program Development

Introduction

Formal adherence to detailed security standards for electronic information processing systems is necessary for industry and government survival. Security standards are needed because of the amount of information, value of the information, and ease with which the information can be manipulated or moved.

In today's computing environment, most organizations have a written security policy and formal security plans and procedures to guide their employees, as well as their business, is protecting their assets. Marketing, finance, engineering, and management all produce and use data sensitive to the organizations business activities. In addition, within the defense industry, some of this data could be considered classified, requiring even stricter controls for its protection.

OBJECTIVES OF A DATA SECURITY PROGRAM

Insure the accuracy and integrity of data.

Insure the protection of classified and sensitive data.

Insure organizational survival in a disaster.

Insure employees understand their responsibilities.

Provide for management awareness.

Provide for a quick response in the event of a compromise.

Setting aside the classification issue for the moment, an organizational policy statement is considered the cornerstone of any effective program for managing and controlling an organization's information assets.[1] Policies are the general plans made by management for providing information and direction. They establish the basic philosophy of the organization and determine the areas where controls must be established. The Data Security Policy is used to support the development of subsequent security procedures. According to Peltier, a good infosecurity program policy statement must do a number of things:

POLICY STATEMENT

The policy statement should be short, easy to read, and not incorporate technical terms.

It must be unambiguous so no one can be exempted from its requirements.

1. Identify information assets.
2. Define who is responsible for classifying and valuing information assets and who must comply.
3. Describe the role of employees in protecting information.
4. Provide for monitoring and enforcement.

In identifying what is to be protected, describe what information is important and what must be

[1] ***Designing Information Security Policies That Get Results***, *Peltier, Thomas R., Infosecurity News, March/April 1993.*

controlled. Begin with a strong sentence describing as completely as possible just what this policy is intended to protect.

Responsibilities should address all levels of the organizational structure, stating who is responsible for complying with the policy and who is responsible for making sure that the classifying policies are enforced. Each employee's security role is spelled out.

Monitoring and enforcement address when the policy take effect, where the policy enforced, and how it will be monitored. For instance, does it apply only for a specific group of employees while in the organization's facilities, or does it apply on travel or in the field. Normally, the question of why the policy was developed is answered in this section also.

The policy statement should be short, easy to read, and not incorporate technical terms. It must also be unambiguous, so that no one can be exempted from the requirements.

Program Responsibility

The ultimate responsibility of a data security program is primarily managements. All levels of management must be involved to insure the program is understood and properly implemented. Management must understand that they are legally responsible for the accuracy and integrity of corporate data.

Employees must recognize that the corporate data on their computers is both valuable and sensitive to the corporation. They must also understand their legal responsibilities regarding the unauthorized release of sensitive data. Note that sensitive data means data that requires protection due to the risk and magnitude of loss or harm that could result from its disclosure, alteration, or destruction.

The following table summarizes the program responsibilities for various levels within the corporation:

1. Chairman of the Board

   To protect and insure for continuity of the corporation

2. Managers

   To maintain information as a strategic asset of the corporation

3. ADP Security Manager

   Must insure written policies and procedures are developed, implemented and followed

4. Users

   Ultimate responsibility for accidental or intentional destruction or disclosure

Recognizing the Problem

If management and employees each understand their responsibilities for protecting computer data, it follows that they must also recognize the problems they face. Four issues must be considered:

1. A business risk is anything that could potentially harm the operation, assets, or

profitability of the organization. The risk analysis is the formal process of determining where exposures could occur and how much potential harm they could cause. For each exposure, the risk analysis performs a cost-benefit analysis to determine if the cost to implement protection is justified by the cost of the assets loss.

2. Vulnerability, in general, relates to the safety of tangible assets in the corporation, and how likely these assets are to being exploited. Obviously, the weakest link in the security chain is also the most vulnerable point. Since the three basic goals of computer security are ensuring secrecy, integrity, and availability of data, vulnerabilities of a computer oriented business can include just about everything related to the business operation. Typical assets are hardware, software, data files, support documentation, people, and outside communications.

3. Motivation is a very flexible and personal concept. What is a strong motivation for one person might not have any effect at all on another. The disgruntled employee who imports or develops a virus does so for revenge. Crackers that break into protected networks or sensitive files could be motivated by peer pressure or simply entertainment. Spies could be driven by political or financial reasons. Regardless of motivation, the personal perspectives of individuals who have access to corporate computing assets are of critical importance.

4. Opportunity is closely tied to motivation. Those individuals who have access to corporate computing assets are those who have the opportunity to create problems. The three basic requirements of data security are secrecy, integrity and availability. Opportunity, or more correctly access control, is therefore the foundation of security for computing systems.

Program Security Objectives

Before discussing the components of a comprehensive data security program, it is appropriate to consider the objectives of such a program. There are really two types of objectives, people protection and data protection. These information systems security objectives can be simplified in the following generic list:

1. Prevention (active measures)
2. Protection (direct protection, rule enforcement, redundancy)
3. Detection (unauthorized disclosures and access)
4. Damage Assessment (timely and accurate assessment)
5. Recovery (procedures)

Below is a typical list of program objectives that would guide the development of an overall security program for people. These objectives would normally be incorporated into the Data Security Policy document and would also appear to some extent in the security plans and procedures documentation.

1. Guard against and remove from unnecessary temptation the misuse data that

employees might be exposed to while fulfilling job responsibilities.

2. Ensure management awareness of the need for security, and their participation in the development and implementation of security policies.
3. Insure the accuracy and integrity of data.
4. Insure the protection of sensitive or confidential data.
5. Provide protection from acts that would cause either hardware or program malfunctions, errors and omissions, or the unauthorized disclosure or destruction of data.
6. Insure the controls and procedures are in place that allow immediate detection and identification of computer security threats to sensitive data.
7. Protect management from charges of imprudence in the event of any compromise of data security.
8. Insure the ability of the organization to survive business interruptions and function adequately after survival.

Data security objectives are included in security policy and procedure documentation. These objectives are much more rule oriented and direct, often addressing specific systems or equipment.

1. Active measures to prevent unauthorized disclosure of protected information.
2. Overall protection includes a combination of direct protection, strict rule enforcement, and redundancy in coverage and backup.
3. Measures to allow for real time detection of unauthorized disclosures and access.
4. Timely and accurate assessment of damage following detection, physical penetration, or disaster.
5. Orderly procedures for returning information processing capabilities to full operation following a disaster.

Developing the Security Program

While data security programs are sometimes implemented following an actual loss or incident, most prudent business organizations address security early in their corporate life. Typically, the concern for physical security best understood and is therefore addressed first. However, if the corporation depends on data processing needs, a comprehensive data security program covering computing issues will soon follow.

The typical areas a security program might include are identified below:

Physical Security: Prudent measures to provide for physical security include the installation of appropriate fire-rated walls, physical access controls to the facility and processing areas, automatic fire detection and extinguishment systems.

Contingency Plan (Disaster Recovery Plan): This aspect of a security plan is based on the realization that if a disaster occurred, the organization must be able to resume its critical processing. It requires the identification of those applications critical to survival, e.g.,

storage of the related operating systems, operator instructions, utilities, programs, and data in an off-site storage facility. The most crucial aspect of this program is auditing (testing) the plan using the designated alternate processing site.

Protected Data Controls: Aside from personnel, the most vital computer-related assets are programs and data. They must be protected by proper identification and authentication of the user. Properly controlled, this will insure that the user is who he purports to be and that he is authorized to have access to the data. This control ultimately resides at the disk level, but includes all computer security threats: interruption, interception, modification, and fabrication.

Network Security: Modern networking systems have evolved into a highly technical discipline. Many organizations rely heavily on these systems to communicate and gather information. Because of this dependency, network systems normally require special security, contingency plans, and data access controls of their own.

Each of the above areas are critical for the overall security program posture, and each are covered in formal security plans and procedures. However, the protected data controls area and the network security area set the baseline for formal ADP Security programs, and are usually combined into the overall ADP Security Plan for a corporation.

Conclusion

This chapter has addressed the principal program management needs objectives in developing a corporate security policy. It has also sets the stage for the subsequent development of the formal computing security plan, the Disaster Recovery Plan, and the procedures governing corporate physical security safeguards. Each organization has its own different and unique computing needs and corporate objectives. Merging these concepts to allow easy acceptance of security controls, while at the same time fully protecting the corporation's computer information assets, is no simple task.

Bibliography

Pfleeger, Charles P., **Security in Computing**, Prentice Hall, Englewood Cliffs, New jersey 07632

Data Security Concepts

The data resident in computer systems is vulnerable. Vulnerabilities also extend to the communication between computers in networks. Computer threats are circumstances that could cause loss or destruction of data. Security breaches also can include exposure through disclosure, modification, or access denial to legitimate users. In general, there are four kinds of computer security threats: interruption, interception, modification and fabrication.

Interruptions occur through file or equipment destruction in which the data becomes lost or unusable. Viruses imported into a system are a common cause of data destruction.

Interceptions are any unauthorized access which may or may not result in the illicit use of data. Both reviewing stored files and monitoring transferred are considered access. Network crackers constantly break into systems using software techniques. Hardwiring a data recorder into a phone system or using a sniffer in a network might be considered hardware techniques to gain access.

Modification includes tampering with information once access has been achieved by changing software or hardware controls or the data itself.

Fabrication is the practice of skillfully adding data or objects to the computing system such as transactions or additional files on a database. An example of data tampering would be accessing a university data base to change the grade received in a class.