COMPUTER SECURITY POLICY

CSL Bulletin
January 1994

SETTING THE STAGE FOR SUCCESS

Executives and managers are faced with many choices in directing the protection of computer assets. Some choices can be based upon quantifiable tradeoffs, but others involve competing tradeoffs, questions of organizational strategic direction, or other parameters which do not lend themselves to quantitative analysis. In making these choices, policy is established for an organization and is then used as the basis for protecting resources, both information and technology, and guiding employee behavior.

Familiarity with various types of policy will aid managers in addressing computer security issues important to the organization. Effective policies ultimately result in the development and implementation of a better computer security program and better protection of systems and information.

This CSL Bulletin discusses four types of computer security policy, their components, and aspects of policy implementation. Program-level policy is used to create an organization's computer security program. Program-framework policy establishes the organization's overall approach to computer security (i.e., its computer security framework). Issue-specific policies address specific issues of concern to the organization. Lastly, system-specific policies focus on policy issues which management has decided for a specific system. Comparison of an organization's computer security policies to the types described in this bulletin will assist managers in determining if their policies are comprehensive and appropriate.

*****SIDEBAR: This bulletin summarizes a chapter of a computer security handbook being developed by CSL. In August 1993, we presented a discussion of the establishment and operation of a computer security program. Our October 1993 bulletin on "People: An Important Asset in Computer Security" summarized another handbook chapter. Additional bulletins will be issued as chapters are finalized. END SIDEBAR

Types of Computer Security Policy

Organizations need program-level policy to establish the security program, assign program management responsibilities, state organization-wide computer security purpose and objectives, and provide a basis for compliance. Program-level policy is typically issued by the head of the organization or another senior official, such as the top management officer.

Program-framework policies provide organization-wide direction on broad areas of program implementation. For example, they may be issued to assure that all components of an organization address contingency planning or risk analysis. They are appropriate when an organization can yield benefits from a consistent approach. Program-framework policies are issued by a manager with sufficient authority to direct all organization components on computer security issues. This may be the organization's management official or the head of the computer security program.

Issue-specific policies identify and define specific areas of concern and state the organization's position. Depending upon the issue and attendant controversy, as well as potential impact, issue-specific policy may come from the head of the organization, the top management official, the Chief Information Officer, or the computer security program manager.

System-specific policies state the security objectives of a specific system, define how the system should be operated to achieve the security objectives, and specify how the protections and features of the technology will be used to support or enforce the security objectives. A system refers to the entire collection of processes, both automated and manual. System-specific policy is normally issued by the manager or owner of the system (which could be a network or application), but may originate from a high official, particularly if all impacted organizational elements do not agree with the new policy.

*******SIDEBAR**

Tools to Implement Policy: Standards, Guidelines, and Procedures Because policy is written at a broad level, organizations also develop standards, guidelines, and procedures which offer users, managers, and others a clearer approach to implementing policy and meeting organizational goals. Standards and guidelines specify technologies and methodologies to be used to secure systems. Procedures are yet more detailed steps to be followed to accomplish particular security-related tasks. Standards, guidelines, and procedures may be disseminated throughout an organization via handbooks, regulations, or manuals.

Organizational standards specify uniform use of specific technologies, parameters, or procedures when such uniform use will benefit an organization. Standardization of organization-wide identification badges is a typical example, providing ease of employee mobility and automation of entry/exit systems. Standards are normally compulsory within an organization.

Guidelines assist users, systems personnel, and others in effectively securing their systems. The nature of guidelines, however, immediately recognizes that systems vary considerably and imposition of standards is not always achievable, appropriate, or cost-effective. An organization guideline may, for example, be used to help develop system-specific standard procedures. Guidelines are often used to help ensure that specific security measures are not overlooked, although they can be implemented, and correctly so, in more than one way.

security policies

Procedures normally assist in complying with applicable security policies, standards, and guidelines. They are detailed steps to be followed by users, system operations personnel, or others to accomplish a particular task (e.g., preparing new user accounts and assigning the appropriate privileges).

Some organizations issue overall computer security “manuals,” “regulations,” “handbooks,” or similar documents. These may mix policy, guidelines, standards, and procedures, since they are closely linked. While manuals and regulations can serve as important tools, they are most useful when they clearly distinguish between policy and its implementation (sometimes a difficult process). This promotes flexibility and cost- effectiveness by offering alternative implementation approaches to achieving policy goals. ***** END SIDEBAR

Program-Level Policy

Program-level policy establishes the computer security program and its basic framework. This high-level policy defines the purpose of the program and its scope within the organization, assigns responsibilities for direct program implementation (to the computer security organization) as well as responsibilities to related offices (such as the IRM organization), and addresses compliance issues. Components of program-level policy should include:

Purpose

Clearly states the purpose of the program. This includes defining the goals of the computer security program as well as its management structure. Security-related needs, such as integrity, availability, and confidentiality, can form the basis of organizational goals established in policy. For instance, in an organization responsible for maintaining large mission-critical databases, reduction in errors, data loss, or data corruption might be specifically stressed. In an organization responsible for maintaining confidential personal data, however, goals might emphasize stronger protection against unauthorized disclosure.

The program management structure should be organized to best address the goals of the program and respond to the particular operating and risk environment of the organization. Important issues for the structure of the central computer security program include management and coordination of security-related resources, interaction with diverse communities, and the ability to relay issues of concern to upper management. The policy could also establish operational security offices for major systems, particularly those at high risk or most critical to organizational operations.

Scope

Specifies which resources (including facilities, hardware, and software), information, and personnel the program covers. In many cases, the program will cover all systems and agency personnel, but this is not always true. In some instances, a policy may name specific assets, such as major sites and large systems. Often tough management decisions arise when defining the scope of a program, such as determining the extent to which the program applies to contractors and outside organizations utilizing or connected to the organization's systems. The Computer Security Act of 1987 requires federal agencies to address the security of all federal interest systems.

Responsibilities

Addresses the responsibilities of officials and offices throughout the organization, including the role of line managers, applications owners, users, and the data processing or IRM organization. The policy statement should distinguish between the responsibilities of computer services providers and the managers of applications utilizing the computer services. It can also serve as the basis for establishing employee accountability. Overall, the program-level assignment of responsibilities should cover those activities and personnel who will be integral to the implementation and continuity of the computer security policy.

Compliance

Authorizes the use of specified penalties and disciplinary actions for individuals who fail to comply with the organization's computer security policies. Since the security policy is a high-level document, penalties for various infractions are normally not detailed here. However, the policy may authorize the creation of compliance structures which include violations and specific penalties. Infractions and associated penalties are usually defined in issue-specific and system-specific policies.

When establishing compliance structures, consider that violations of policy can be unintentional on the part of employees. For example, nonconformance can be due to a lack of knowledge or training.

Program-Framework Policy

Program-framework policy defines the organization's security program elements which form the framework for the computer security program and reflect decisions about priorities for protection, resource allocation, and assignment of responsibilities.

Criteria for the types of areas to be addressed as computer security program elements include, but are not limited to:

_areas for which there is an advantage to the organization by having the issue addressed in a common manner;

_areas which need to be addressed for the entire organization;

_areas for which organization-wide oversight is necessary; and

_areas which, through organization-wide implementation, can yield significant economies of scale.

The types of areas addressed by program-framework policy vary within each organization as does the way in which the policy is expressed. Some organizations issue policy directives, while others issue handbooks which combine policy, regulations, standards, and guidance. Many organizations issue policy on "key" areas of computer security, such as life cycle management, contingency planning, and network security.

Keep in mind the criteria stated above for the types of areas that should be addressed in program-framework policy. If the policy (and its implementing standards and guidance) is too rigid, cost-effective implementations and innovation could be stifled.

As an example of program-framework policy, consider a typical organization policy on contingency planning. The organization might require that all contingency plans categorize criticality of processing according to a standard scale. This will assist the organization in the preparation of a master plan (for use if the organization's physical plant is destroyed) by facilitating prioritization across intra-organizational boundaries.

Policy in these areas normally applies throughout the organization and is usually independent of technology and the system or application. Program-framework policies may be comprised of components similar to those contained in program-level policy—but may be in a very different format (e.g., in organizational handbook directives).

Issue-Specific Policy

Issue-specific policies focus on areas of current relevance and concern (and sometimes controversy). Program-level policy is usually broad enough that it requires little modification over time. Conversely, issue-specific policies require more frequent revision due to changes in technology and related factors. As new technologies develop, some issues diminish in importance while new ones continually appear. It may be appropriate, for example, to issue a policy on the proper use of a cutting-edge technology, the security vulnerabilities of which are still largely unknown.

A useful structure for issue-specific policy is to break the policy into its basic components: statement of an issue, statement of the organization's position, applicability, roles and responsibilities, compliance, and points of contact. Other topic areas may be added as needed.

Issue Statement

Defines the issue, with any relevant terms, distinctions, and conditions. For example, an organization might want to develop an issue-specific policy on the use of "unapproved software," which might be defined to mean any software not approved, purchased, screened, managed, and owned by the organization. Additionally, applicable distinctions and conditions might need to be included, for instance, software privately owned by employees but approved for use at work and for software owned and used by other businesses under contract to the organization.

Statement of the Organization's Position

Clearly states the organization's position on the issue. To continue the example of unapproved software, the policy would state whether use of unapproved software is prohibited in all or some cases, whether or not there are further guidelines for approval and use, or whether case-by-case exceptions will be granted, by whom, and on what basis.

Applicability

Clearly states where, how, when, to whom, and to what a particular policy applies. For example, the hypothetical policy on unapproved software may apply only to the organization's own on-site resources and employees and not to contractor organizations with offices at other locations. Additionally, the policy's applicability to employees travelling among different sites or working at home who will transport and use disks at multiple sites might require clarification.

Roles and Responsibilities

Assigns roles and responsibilities. To continue the software example, if the policy permits unapproved software privately owned by employees to be used at work with appropriate approvals, then the approving authority would be identified. An office responsible for compliance could also be named.

Compliance

Gives descriptions of the infractions which are unacceptable and states the corresponding penalties. Penalties must be consistent with organizational personnel policies and practices and need to be coordinated with appropriate officials, offices and, perhaps, employee bargaining units.

Points of Contact and Supplementary Information

Gives the name of the appropriate individuals to contact for further information and lists any applicable standards or guidelines. For some issues the point of contact might be a line manager; for other issues it might be a facility manager, technical support person, or system administrator. For yet other issues, the point-of-contact might be a security program representative. Using the software example, employees need to know whether the point of contact for questions and procedural information would be the immediate superior, a system administrator, or a computer security official.

System-Specific Policy

Program-level policy and issue-specific policy both address policy from a broad level, usually encompassing the entire organization. System-specific policy, on the other hand, is much more focused, since it addresses only one system.

Many security policy decisions apply only at the system level.

Some examples include:

_Who is allowed to read or modify data in the system?
_Under what conditions can data be read or modified?
_Are users allowed to dial into the computer system from home or while on travel?

To develop a comprehensive set of system security policies, use a management process which derives security rules from security goals. Consider a three-level model for system security policy: security objectives, operational security, and policy implementation.

Security Objectives

First, define security objectives. While this process may start with an analysis of the need for integrity, availability, and confidentiality, it cannot stop there. A security objective must be more specific, concrete, and well-defined. It also should be stated so that it is clear that the objective is achievable.

The security objectives should consist of a series of statements which describe meaningful actions about specific resources. These objectives should be based on system functional or mission requirements, but should state the security actions which support the requirements.

Operational Security

Next lay out the operational policy which gives the rules for operating a system. Following the same integrity example, the operational policy would define authorized and unauthorized modification: who, (by job category, by organization placement, or by name) can do what (modify, delete, etc.) to which pieces of data (specific fields or records) and under what conditions.

Managers need to make decisions in developing this policy since it is unlikely that all security objectives will be fully met. Cost, operational, technical, and other constraints will intervene.

Consider the degree of granularity needed for operational security policies. Granularity refers to how specific the policy is with regard to resources or rules. The more granular the policies, the easier to enforce and to detect violations. A policy violation may indicate a security problem. In addition, the more granular the policy, the easier to automate policy enforcement.

Consider the degree of formality you want in documenting the policy. Once again, the more formal the documentation, the easier to enforce and to follow policy. Formal policy is published as a distinct policy document; less formal policy may be written in memos. Informal policy may not be written at all. Unwritten policy is extremely difficult to follow or enforce.

On the other hand, very granular and formal policy at the system level can also be an administrative burden. In general, good practice suggests a granular formal statement of the access privileges for a system due to its complexity and importance. Documenting access controls policy makes it substantially easier to follow and to enforce. Another area that normally requires a granular and formal statement is the assignment of security responsibilities.

Some less formal policy decisions may be recorded in other types of computer security documents such as risk analyses, accreditation statements, or procedural manuals. However, any controversial, atypical, or uncommon policies may need formal policy statements. Atypical policies would include any areas where the system policy is different from organization policy or from normal practice within the organization, either more or less stringent. They should also contain a statement explaining the reason for deviation from the organization’s standard policy.

Policy Implementation

Determine the role technology will play in enforcing or supporting the policy. Security is normally enforced through a combination of technical and traditional management methods.

While technical means are likely to include the use of access control technology, there are other automated means of enforcing or supporting security policy. For example, technology can be used to block telephone systems users from calling certain numbers. Intrusion detection software can alert system administrators to suspicious activity or take action to stop the activity. Personal computers can be configured to prevent booting from a floppy disk.

Automated security enforcement has advantages and disadvantages. A computer system, properly designed, programmed, and installed, consistently enforces policy, although no computer can force users to follow all procedures. In addition, deviations from the policy may sometimes be necessary and appropriate. This situation occurs frequently if the security policy is too rigid.

Helpful Hints

To be effective, policy requires visibility. Visibility aids implementation of policy by helping to ensure that knowledge of the policy is diffused throughout the organization. Use management presentations, videos, panel discussions, guest speakers, question/answer forums, and newsletters, as resources permit. The organization's computer security training and awareness program can effectively notify users of new policies.

Introduce computer security policies in a manner that ensures that management's unqualified support is clear, especially in environments where employees feel inundated with policies, directives, guidelines, and procedures. The organization's policy is the vehicle for emphasizing management's commitment to computer security and making clear their expectations for employee performance, behavior, and accountability.

Computer security policy should also be integrated into and consistent with other organizational policies, such as personnel policies). One way to help ensure this is to thoroughly coordinate policies during development with other offices in the organization.

Conclusion

Formulating viable computer security policies is a challenge for an organization and requires communication and understanding of the organizational goals and potential benefits to be derived from policies. Through a carefully structured approach to policy development, which includes the delegation of program management responsibility and an understanding of program-level, program- framework, issue-specific, and system-specific policy components, your organization can achieve a coherent set of policies. These will help produce a framework for a successful computer security program.