Chapter 5

COMPUTER SECURITY POLICY

In discussions of computer security, the term *policy* has more than one meaning.[45] *Policy* is senior management's directives to create a computer security program, establish its goals, and assign responsibilities. The term *policy* is also used to refer to the specific security rules for particular systems.[46] Additionally, *policy* may refer to entirely different matters, such as the specific managerial decisions setting an organization's e-mail privacy policy or fax security policy.

Policy means different things to different people. The term "policy" is used in this chapter in a broad manner to refer to important computer security-related decisions.

In this chapter the term *computer security policy* is defined as the "documentation of computer security decisions" – which covers all the types of policy described above.[47] In making these decisions, managers face hard choices involving resource allocation, competing objectives, and organizational strategy related to protecting both technical and information resources as well as guiding employee behavior. Managers at all levels make choices that can result in policy, with the scope of the policy's applicability varying according to the scope of the manager's authority. In this chapter we use the term *policy* in a broad manner to encompass all of the types of policy described above – regardless of the level of manager who sets the particular policy.

Managerial decisions on computer security issues vary greatly. To differentiate among various kinds of policy, this chapter categorizes them into three basic types:

- *Program policy* is used to create an organization's computer security program.
- *Issue-specific policies* address specific issues of concern to the organization.

---

[45] There are variations in the use of the term *policy*, as noted in a 1994 Office of Technology Assessment report, *Information Security and Privacy in Network Environments*: "*Security Policy* refers here to the statements made by organizations, corporations, and agencies to establish overall policy on information access and safeguards. Another meaning comes from the Defense community and refers to the rules relating clearances of users to classification of information. In another usage, *security policies* are used to refine and implement the broader, organizational security policy...."

[46] These are the kind of policies that computer security experts refer to as being *enforced* by the system's technical controls as well as its management and operational controls.

[47] In general, policy is set by a manager. However, in some cases, it may be set by a group (e.g., an intraorganizational policy board).

- *System-specific policies* focus on decisions taken by management to protect a particular system.[48]

Procedures, standards, and guidelines are used to describe how these policies will be implemented within an organization. (See following box.)

Tools to Implement Policy:
Standards, Guidelines, and Procedures

Because policy is written at a broad level, organizations also develop standards, guidelines, and procedures that 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 promulgated throughout an organization via handbooks, regulations, or manuals.

Organizational standards (not to be confused with American National Standards, FIPS, Federal Standards, or other national or international standards) specify uniform use of specific technologies, parameters, or procedures when such uniform use will benefit an organization. Standardization of organizationwide 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. For example, an organizational guideline may 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.

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, it is often useful if they clearly distinguish between policy and its implementation. This can help in promoting flexibility and cost-effectiveness by offering alternative implementation approaches to achieving policy goals.

[48] A *system* refers to the entire collection of processes, both those performed manually and those using a computer (e.g., manual data collection and subsequent computer manipulation), which performs a function. This includes both application systems and support systems, such as a network.

Familiarity with various types and components 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 protectio n of systems and information.

These types of policy are described to aid the reader's understanding.[49] It is not important that one categorizes specific organizational policies into these three categories; it is more important to focus on the functions of each.

5.1 Program Policy

A management official, normally the head of the organization or the senior administration official, issues program policy to establish (or restructure) the organization's computer security program and its basic structure. This high-level policy defines the purpose of the program and its scope within the organization; assigns responsibilities (to the computer security organization) for direct program implementation, as well as other responsibilities to related offices (such as the Information Resources Management [IRM] organization); and addresses compliance issues.

Program policy sets organizational strategic directions for security and assigns resources for its implementation.

5.1.1 Basic Components of Program Policy

Components of program policy should address:

Purpose. Program policy normally includes a statement describing why the program is being established. This may include defining the *goals* of the program. 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, data corruption, and recovery might be specifically stressed. In an organization responsible for maintaining confidential personal data, however, goals might emphasize stronger protection against unauthorized disclosure.

Scope. Program policy should be clear as to which resources -- including facilities, hardware, and software, information, and personnel -- the computer security program covers. In many cases, the program will encompass all systems and organizational personnel, but this is not always true. In some instances, it may be appropriate for an organization's computer security program to be more limited in scope.

---

[49] No standard terms exist for various types of policies. These terms are used to aid the reader's understanding of this topic; no implication of their widespread usage is intended.

Responsibilities. Once the computer security program is established, its management is normally assigned to either a newly created or existing office.[50]

Program policy establishes the security program and assigns program management and supporting responsibilities.

The responsibilities of officials and offices throughout the organization also need to be addressed, including line managers, applications owners, users, and the data processing or IRM organizations. This section of the policy statement, for example, would distinguish between the responsibilities of computer services providers and those of the managers of applications using the provided services. The policy could also establish operational security offices for major systems, particularly those at high risk or most critical to organizational operations. It also can serve as the basis for establishing employee accountability.

At the program level, responsibilities should be specifically assigned to those organizational elements and officials responsible for the implementation and continuity of the computer security policy.[51]

Compliance. Program policy typically will address two compliance issues:

1. General compliance to ensure meeting the requirements to establish a program and the responsibilities assigned therein to various organizational components. Often an oversight office (e.g., the Inspector General) is assigned responsibility for monitoring compliance, including how well the organization is implementing management's priorities for the program.

2. The use of specified penalties and disciplinary actions. Since the security policy is a high-level document, specific penalties for various infractions are normally not detailed here; instead, the policy may authorize the creation of compliance structures that include violations and specific disciplinary action(s).[52]

---

[50] 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 computer security program include management and coordination of security-related resources, interaction with diverse communities, and the ability to relay issues of concern, trade-offs, and recommended actions to upper management. (See Chapter 6, Computer Security Program Management.)

[51] In assigning responsibilities, it is necessary to be specific; such assignments as "computer security is everyone's responsibility," in reality, mean no one has specific responsibility.

[52] The need to obtain guidance from appropriate legal counsel is critical when addressing issues involving penalties and disciplinary action for individuals. The policy does not need to restate penalties already provided

Those developing compliance policy should remember that violations of policy can be unintentional on the part of employees. For example, nonconformance can often be due to a lack of knowledge or training.

5.2 Issue-Specific Policy

Whereas program policy is intended to address the broad organizationwide computer security program, issue-specific policies are developed to focus on areas of current relevance and concern (and sometimes controversy) to an organization. Management may find it appropriate, for example, to issue a policy on how the organization will approach contingency planning (centralized vs. decentralized) or the use of a particular methodology for managing risk to systems. A policy could also be issued, for example, on the appropriate use of a cutting-edge technology (whose security vulnerabilities are still largely unknown) within the organization. Issue-specific policies may also be appropriate when new issues arise, such as when implementing a recently passed law requiring additional protection of particular information. Program policy is usually broad enough that it does not require much modification over time, whereas issue-specific policies are likely to require more frequent revision as changes in technology and related factors take place.

In general, for issue-specific and system-specific policy, the issuer is a senior official; the more global, controversial, or resource-intensive, the more senior the issuer.

5.2.1 Example Topics for Issue-Specific Policy[53]

Both new technologies and the appearance of new threats often require the creation of issue-specific policies.

There are many areas for which issue-specific policy may be appropriate. Two examples are explained below.

Internet Access. Many organizations are looking at the Internet as a means for expanding their research opportunities and communications. Unquestionably, connecting to the Internet yields many benefits – and some disadvantages. Some issues an Internet access policy may address include who will have access, which types of systems may be connected to the network, what types of information may be transmitted via the network, requirements for user authentication for Internet-connected systems, and the use of firewalls and secure gateways.

---

for by law, although they can be listed if the policy will also be used as an awareness or training document.

[53] Examples presented in this section are not all-inclusive nor meant to imply that policies in each of these areas are required by all organizations.

E-Mail Privacy. Users of computer e-mail systems have come to rely upon that service for informal communication with colleagues and others. However, since the system is typically owned by the employing organization, from time-to-time, management may wish to monitor the employee's e-mail for various reasons (e.g., to be sure that it is used for business purposes only or if they are suspected of distributing viruses, sending offensive e-mail, or disclosing organizational secrets.) On the other hand, users may have an expectation of privacy, similar to that accorded U.S. mail. Policy in this area addresses what level of privacy will be accorded e-mail and the circumstances under which it may or may not be read.

Other potential candidates for issue-specific policies include: approach to risk management and contingency planning, protection of confidential/proprietary information, unauthorized software, acquisition of software, doing computer work at home, bringing in disks from outside the workplace, access to other employees' files, encryption of files and e-mail, rights of privacy, responsibility for correctness of data, suspected malicious code, and physical emergencies.

5.2.2 Basic Components of Issue-Specific Policy

As suggested for program policy, a useful structure for issue-specific policy is to break the policy into its basic components.

Issue Statement. To formulate a policy on an issue, managers first must define the issue with any relevant terms, distinctions, and conditions included. It is also often useful to specify the goal or justification for the policy – which can be helpful in gaining compliance with the policy. For example, an organization might want to develop an issue-specific policy on the use of "unofficial software," which might be defined to mean any software not approved, purchased, screened, managed, and owned by the organization. Additionally, the applicable distinctions and conditions might then need to be included, for instance, for 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. Once the issue is stated and related terms and conditions are discussed, this section is used to clearly state the organization's position (i.e., management's decision) on the issue. To continue the previous example, this would mean stating whether use of unofficial software as defined is prohibited in all or some cases, whether there are further guidelines for approval and use, or whether case-by-case exceptions will be granted, by whom, and on what basis.

Applicability. Issue-specific policies also need to include statements of applicability. This means clarifying where, how, when, to whom, and to what a particular policy applies. For example, it could be that the hypothetical policy on unofficial software is intended to apply only to the organization's own on-site resources and employees and not to contractors with offices at other

locations. Additionally, the policy's applicability to employees travelling among different sites and/or working at home who need to transport and use disks at multiple sites might need to be clarified.

Roles and Responsibilities. The assignment of roles and responsibilities is also usually included in issue-specific policies. For example, if the policy permits unofficial software privately owned by employees to be used at work with the appropriate approvals, then the approval authority granting such permission would need to be stated. (Policy would stipulate, who, by position, has such authority.) Likewise, it would need to be clarified who would be responsible for ensuring that only approved software is used on organizational computer resources and, perhaps, for monitoring users in regard to unofficial software.

Compliance. For some types of policy, it may be appropriate to describe, in some detail, the infractions that are unacceptable, and the consequences of such behavior. Penalties may be explicitly stated and should be consistent with organizational personnel policies and practices. When used, they should be coordinated with appropriate officials and offices and, perhaps, employee bargaining units. It may also be desirable to task a specific office within the organization to monitor compliance.

Points of Contact and Supplementary Information. For any issue-specific policy, the appropriate individuals in the organization to contact for further information, guidance, and compliance should be indicated. Since positions tend to change less often than the people occupying them, specific positions may be preferable as the point of contact. For example, for some issues the point of contact might be a line manager; for other issues it might be a facility manager, technical support person, system administrator, or security program representative. Using the above example once more, employees would need to know whether the point of contact for questions and procedural information would be their immediate superior, a system

Some Helpful Hints on Policy

To be effective, policy requires visibility. Visibility aids implementation of policy by helping to ensure policy is fully communicated throughout the organization. Management presentations, videos, panel discussions, guest speakers, question/answer forums, and newsletters increase visibility. The organization's computer security training and awareness program can effectively notify users of new policies. It also can be used to familiarize new employees with the organization's policies.

Computer security policies should be introduced 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.

To be effective, policy should be consistent with other existing directives, laws, organizational culture, guidelines, procedures, and the organization's overall mission. It should also be integrated into and consistent with other organizational policies (e.g., personnel policies). One way to help ensure this is to coordinate policies during development with other organizational offices.

administrator, or a computer security official.

Guidelines and procedures often accompany policy. The issue-specific policy on unofficial software, for example, might include procedural guidelines for checking disks brought to work that had been used by employees at other locations.

5.3 System-Specific Policy

Program policy and issue-specific policy both address policy from a broad level, usually encompassing the entire organization. However, they do not provide sufficient information or direction, for example, to be used in establishing an access control list or in training users on what actions are permitted. System-specific policy fills this need. It is much more focused, since it addresses only one system.

Many security policy decisions may apply only at the system level and may vary from system to system within the same organization. While these decisions may appear to be too detailed to be policy, they can be extremely important, with significant impacts on system usage and security. These types of decisions can be made by a *management official*, not by a technical system administrator.[54] (The impacts of these decisions, however, are often analyzed by technical system administrators.)

> System-specific security policy includes two components: security objectives and operational security rules. It is often accompanied by implementing procedures and guidelines.

To develop a cohesive and comprehensive set of security policies, officials may use a management process that derives security rules from security goals. It is helpful to consider a two-level model for system security policy: security objectives and operational security rules, which together comprise the system-specific policy. Closely linked and often difficult to distinguish, however, is the implementation of the policy in technology.

5.3.1 Security Objectives

> **Sample Security Objective**
>
> Only individuals in the accounting and personnel departments are authorized to provide or modify information used in payroll processing.

The first step in the management process is to define security objectives for the specific system. Although, this process may start with an analysis of the need for integrity,

[54] It is important to remember that policy is not created in a vacuum. For example, it is critical to understand the system mission and how the system is intended to be used. Also, users may play an important role in setting policy.

availability, and confidentiality, it should not stop there. A security *objective* needs to more specific; it should be concrete and well defined. It also should be stated so that it is clear that the objective is achievable. This process will also draw upon other applicable organization policies.

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

Development of system-specific policy will require management to make trade-offs, since it is unlikely that all desired security objectives will be able to be fully met. Management will face cost, operational, technical, and other constraints.

5.3.2 Operational Security Rules

After management determines the security objectives, the rules for operating a system can be laid out, for example, to define authorized and unauthorized modification. Who (by job category, organization placement, or name) can do what (e.g., modify, delete) to which specific classes and records of data, and under what conditions.

Sample Operational Security Rule

Personnel clerks may update fields for weekly attendance, charges to annual leave, employee addresses, and telephone numbers. Personnel specialists may update salary information. No employees may update their own records.

The degree of specificity needed for operational security rules varies greatly. The more detailed the rules are, *up to a point*, the easier it is to know when one has been violated. It is also, *up to a point*, easier to automate policy enforcement. However, overly detailed rules may make the job of instructing a computer to implement them difficult or computationally complex.

In addition to deciding the level of detail, management should decide the degree of formality in documenting the system-specific policy. Once again, the more formal the documentation, the easier it is to enforce and to follow policy. On the other hand, policy at the system level that is too detailed and formal can also be an administrative burden. In general, good practice suggests a reasonably detailed formal statement of the access privileges for a system. Documenting access controls policy will make it substantially easier to follow and to enforce. (See Chapters 10 and 17, Personnel/User Issues and Logical Access Control.) Another area that normally requires a detailed and formal statement is the assignment of security responsibilities. Other areas that should be addressed are the rules for system usage and the consequences of noncompliance.

Policy decisions in other areas of computer security, such as those described in this handbook, are often documented in the risk analysis, accreditation statements, or procedural manuals. However,

any controversial, atypical, or uncommon policies will also need formal statements. Atypical policies would include any areas where the system policy is different from organizational policy or from normal practice within the organization, either more or less stringent. The documentation for a typical policy contains a statement explaining the reason for deviation from the organization's standard policy.

5.3.3 System-Specific Policy Implementation

Technology plays an important – but not sole – role in enforcing system-specific policies. When technology is used to enforce policy, it is important not to neglect nontechnology- based methods. For example, technical system-based controls could be used to limit the printing of confidential reports to a particular printer. However, corresponding physical security measures would also have to be in place to limit access to the printer output or the desired security objective would not be achieved.

Technical methods frequently used to implement system-security policy are likely to include the use of *logical access controls*. However, there are other automated means of enforcing or supporting security policy that typically supplement logical access controls. For example, technology can be used to block telephone users from calling certain numbers. Intrusion-detection software can alert system administrators to suspicious activity or can take action to stop the activity. Personal computers can be configured to prevent booting from a floppy disk.

Technology-based enforcement of system-security policy has both advantages and disadvantages. A computer system, properly designed, programmed, installed, configured, and maintained,[55] consistently enforces policy within the computer system, although no computer can force users to follow all procedures. Management controls also play an important role – and should not be neglected. In addition, deviations from the policy may sometimes be necessary and appropriate; such deviations may be difficult to implement easily with some technical controls. This situation occurs frequently if implementation of the security policy is too rigid (which can occur when the system analysts fail to anticipate contingencies and prepare for them).

5.4 Interdependencies

Policy is related to many of the topics covered in this handbook:

Program Management. Policy is used to establish an organization's computer security program, and is therefore closely tied to program management and administration. Both program and system-specific policy may be established in any of the areas covered in this handbook. For

[55] Doing all of these things properly is, unfortunately, the exception rather than the rule. Confidence in the system's ability to enforce system-specific policy is closely tied to assurance. (See Chapter 9, Assurance.)

example, an organization may wish to have a consistent approach to incident handling for all its systems – and would issue appropriate program policy to do so. On the other hand, it may decide that its applications are sufficiently independent of each other that application managers should deal with incidents on an individual basis.

Access Controls. System-specific policy is often implemented through the use of access controls. For example, it may be a policy decision that only two individuals in an organization are authorized to run a check-printing program. Access controls are used by the system to implement (or enforce) this policy.

Links to Broader Organizational Policies. This chapter has focused on the types and components of computer security policy. However, it is important to realize that *computer* security policies are often *extensions* of an organization's *information* security policies for handling information in other forms (e.g., paper documents). For example, an organization's e-mail policy would probably be tied to its broader policy on privacy. Computer security policies may also be extensions of other policies, such as those about appropriate use of equipment and facilities.

5.5 Cost Considerations

A number of potential costs are associated with developing and implementing computer security policies. Overall, the major cost of policy is the cost of implementing the policy and its impacts upon the organization. For example, establishing a computer security program, accomplished through policy, does not come at negligible cost.

Other costs may be those incurred through the policy development process. Numerous administrative and management activities may be required for drafting, reviewing, coordinating, clearing, disseminating, and publicizing policies. In many organizations, successful policy implementation may require additional staffing and training – and can take time. In general, the costs to an organization for computer security policy development and implementation will depend upon how extensive the change needed to achieve a level of risk acceptable to management.

References

Howe, D. "Information System Security Engineering: Cornerstone to the Future." *Proceedings of the 15th National Computer Security Conference*. Baltimore, MD, Vol. 1, October 15, 1992. pp. 244-251.

Fites, P., and M. Kratz. "Policy Development." *Information Systems Security: A Practitioner's Reference*. New York, NY: Van Nostrand Reinhold, 1993. pp. 411-427.

Lobel, J. "Establishing a System Security Policy." *Foiling the System Breakers*. New York, NY: McGraw-Hill, 1986. pp. 57-95.

Menkus, B. "Concerns in Computer Security." *Computers and Security*. 11(3), 1992. pp. 211-215.

Office of Technology Assessment. "Federal Policy Issues and Options." *Defending Secrets, Sharing Data: New Locks for Electronic Information*. Washington, DC: U.S Congress, Office of Technology Assessment, 1987. pp. 151-160.

Office of Technology Assessment. "Major Trends in Policy Development." *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*. Washington, DC: U.S. Congress, Office of Technology Assessment, 1987. p. 131-148.

O'Neill, M., and F. Henninge, Jr. "Understanding ADP System and Network Security Considerations and Risk Analysis." *ISSA Access*. 5(4), 1992. pp. 14-17.

Peltier, Thomas. "Designing Information Security Policies That Get Results." *Infosecurity News*. 4(2), 1993. pp. 30-31.

President's Council on Management Improvement and the President's Council on Integrity and Efficiency. *Model Framework for Management Control Over Automated Information System*. Washington, DC: President's Council on Management Improvement, January 1988.

Smith, J. "Privacy Policies and Practices: Inside the Organizational Maze." *Communications of the ACM*. 36(12), 1993. pp. 104-120.

Sterne, D. F. "On the Buzzword `Computer Security Policy.'" In *Proceedings of the 1991 IEEE Symposium on Security and Privacy*, Oakland, CA: May 1991. pp. 219-230.

Wood, Charles Cresson. "Designing Corporate Information Security Policies." *DATAPRO Reports on Information Security*, April 1992.