Computer and Information Security Policy

* * * * * * * * * * * * * NOTE * * * * * * * * * * * * * * * * *

This file is a DRAFT chapter intended to be part of the NIST Computer Security Handbook. The chapters were prepared by different parties and, in some cases, have not been reviewed by NIST. The next iteration of a chapter could be SUBSTANTIALLY different than the current version. If you wish to provide comments on the chapters, please email them to roback@ecf.ncsl.gov or mail them to Ed Roback/Room B154, Bldg 225/NIST/Gaithersburg, MD 20899.

* *

DRAFT DRAFT DRAFT DRAFT

Introduction to Computer Security Policy

Organizations rely on IT resources today to handle vast amounts of information. Because the data can vary widely in type and in degree of sensitivity, employees need to be able to exercise flexibility in handling and protecting it. It would not be practical or cost-effective to require that all data be handled in the same manner or be subject to the same protection requirements. Without some degree of standardization, however, inconsistencies can develop that introduce risks.

Formal IT security policy helps establish standards for IT resource protection by assigning program management responsibilities and providing basic rules, guidelines, and definitions for everyone in the organization. Policy thus helps prevent inconsistencies that can introduce risks, and policy serves as a basis for the enforcement of more detailed rules and procedures. Ideally, policy will be sufficiently clear and comprehensive to be accepted and followed throughout the organization yet flexible enough to accommodate a wide range of data, activities, and resources.

Policy formulation is an important step toward standardization of security activities for IT resources. IT security policy is generally formulated from the input of many members of an organization, including security officials, line managers, and IT resource specialists. However, policy is ultimately approved and issued by the organization's senior management. In environments where employees feel inundated with policies, directives, guidelines and procedures, an IT security policy should be introduced in a manner that ensures that management's unqualified support is clear. The organization's policy is management's vehicle for emphasizing the commitment to IT security and making clear the expectations for employee involvement and accountability.

This chapter will discuss IT security policy in terms of the different types (program-level and issue-specific), components, and aspects of implementation. Potential cost and interdependencies will also be noted.

Policy Types: Program-Level and Issue-Specific

Two types of policy will typically need to be developed to meet an organization's needs: program-level and issue-specific. Program-level policy's main function is to establish the security program, assign program management responsibilities, state the organizationwide IT security goals and objectives, and provide a basis for enforcement. Issue-specific policies also need to be developed, in order to identify and define specific areas of concern and to state the organization's position and expectations in relation to them. Following are discussions on these two basic types of policy.

Program-level Policy

As discussed above, program-level policy is broad in scope and far-reaching in applicability. To make the subject more manageable, an effective approach to a discussion of program-level IT security policy is to break general policy into its basic components: purpose, scope, goals, responsibilities, and enforcement.

Components of Program-level Policy

Purpose: A primary purpose of program-level policy is to establish the IT security program. This includes defining the program management structure, the reporting responsibilities, the roles of individuals and groups throughout the organization, and the organizationwide goals of the security program. (Chapter 5 provides a detailed discussion of security program management and administration.)

Additionally, program-level policy should serve the purpose of emphasizing to all employees the importance of IT security and clarifying the individual employee's role and responsibilities. IT security policy may be met with a degree of skepticism unless given appropriate visibility and support by top management, and that visibility and support should be clearly and energetically reflected in the program-level policy and in its emphasis on employee participation.

The program-level policy should thus firmly establish individual employee accountability. Employees should be made aware via the policy that even if they are not designated IT security program personnel, they nonetheless have significant IT security responsibilities.

Scope: Program-level policy should be of sufficient breadth of scope to include all of the organization's IT resources, including facilities, hardware, software, information, and personnel. In some instances, it may be appropriate for a policy to name specific assets, such as major sites, installations, and large systems. In addition to such specified assets, it is important to include an overview of all of the types of IT resources for which the organization is responsible, such as workstations, Local Area Networks (LANs), standalone microcomputers, etc.

Goals: According to the National Research Council's Computers at Risk, published in 1991, the three security-related needs universally most emphasized among IT resource experts and the general computer user community are integrity, availability, and confidentiality. These concepts are the focus of many discussions in this handbook as well. These concepts should be the basis of the goals established for an organization in its IT security policy. Integrity means assuring that information is kept intact, and not lost, damaged, or modified in an authorized manner. Availability means assuring that information is accessible to authorized users when needed and that, to the extent possible, IT systems are safe from accidental or intentional disablement. Confidentiality means assuring that information is accessible only as authorized and that it cannot be acquired by unauthorized personnel and/or via unauthorized means.

Goals related to these concepts should be stated in meaningful ways to employees based on the given environment. It is important that the organization's program-level policy reflect goals that are applicable to the specific environment by targeting the kinds of activities, information, and terminology that employees are familiar with.

For instance, in an organization responsible for maintaining large but not highly confidential databases, goals related to reduction in errors, data loss, or data corruption might be specifically stressed. In an organization responsible for maintaining much more confidential data, however, goals might emphasize increased assurance against unauthorized disclosure.

Responsibilities: As noted in the earlier discussion of Purpose, program-level policy performs the important function of establishing the IT security program and assigning program management responsibilities. In addition to the security program management responsibilities, many other responsibilities throughout the organization should also be discussed in the policy, including the role of line managers, applications owners, data users, and the computer systems security group.

In some instances, the relationships among various individuals and groups may also need to be defined in the program-level policy. Such clarification can diminish ambiguity and confusion related to areas of responsibility or authority. It might be desirable to clarify, for example, who is to be responsible for approving the security measures to be used for new systems or components being installed: Should it be the department line manager where the item will be installed? Or should it be a designated inter-departmental IT security specialist? It might even be desirable to indicate under what circumstances, if any, approval of security measures implemented would be warranted by the head of the security program.

Overall, the program-level assignment of responsibilities should cover those activities and personnel who will be integral to the implementation and continuity of the IT security policy.

Enforcement: Without a formal, documented IT security policy, it is not possible for management to proceed with the development of enforcement standards and mechanisms. Program-level policy serves as the basis for enforcement by describing penalties and disciplinary actions that can result from failure to comply with the organization's IT security requirements. Discipline commensurate with levels and types of security infractions should be discussed. For example, serious offenses, such as theft, conspiracy, or intentional acts of sabotage, might be designated by policy as punishable by firing and prosecution. Lesser infractions, such as pirating software, might be stated as punishable by formal written reprimand.

Consideration should also be given to the fact that nonconformance to policy can be unintentional on the part of employees. For example, nonconformance can often be due to a lack of knowledge or training. It can also be the result of inadequate communication and explanation of the policy. For these reasons, it is desirable that, along with enforcement, program-level policy make provisions for orientation, training, and compliance within a realistic timeframe.

Issue-specific Policy

Whereas program-level policy is intended to address the broadest aspects of IT security and the IT security program framework, issue-specific policies need to be developed to address particular kinds of activities and, in some environments, particular systems. The types of subjects covered by issue-specific policies are areas of current relevance, concern, and, sometimes, controversy upon which the organization needs to assert a position. In this manner, issue-specific IT security policies help to standardize activities and reduce the potential risks posed by inadequate and/or inappropriate treatment of the IT resources. Issue-specific policies serve to provide guidelines for the further development of procedures and practices within the functional elements of an organization.

Program-level policy is usually broad enough that it does not require much modification over time. Issue-specific policies, however, are likely to require revision and updating from time to time, as changes in technology and related activities take place. This is largely because as new technologies develop, some issues diminish in importance while new ones continually appear. A major challenge to IT security specialists has long been the fact that for every new technology there are also new associated problems and issues to be addressed.

For example, the enormous increase in the use of electronic mail (E-mai) systems in recent years has introduced many new issues in communications security, which is one of the topics that will be briefly discussed later in this section. Many organizations today are developing and refining communications security policies in order to better address such questions as who should have E-mail access, how will privileges be assigned and monitored, for what types of activities and information is E-mail sufficiently secure, and what criteria should be used for the re-sending (forwarding) of messages among users.

Another topic of recent notoriety impacting IT security policies is the threat posed by computer viruses. New viruses and new methods of transmitting them are making it necessary that organizations develop policies regulating activities that were once performed freely, such as exchanging floppy disks among users, accessing electronic bulletinboards, and using shareware products.

As for the discussion of program-level policy, a useful approach is to first break issue-specific policy into its basic components: statement of an issue, statement of the organization's position, applicability, roles and responsibilities, and points of contact. Thereafter, some of the areas that often require issue-specific policies will be covered.

Components of Issue-specific Policy

Statement of an Issue: In order to formulate a policy on an issue, the issue must first be defined, with any relevant terms, distinctions, and conditions delineated. For example, an organization might want to develop an issue-specific policy on the use of "foreign software." "Foreign software" might be defined to mean any software, whether applications or data, 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 delineated, the organization's position or stance on the issue will need to be clearly stated. To continue the example of developing an issue-specific policy on the use of foreign software, this would mean stating whether use of foreign software as defined is strictly prohibited, whether or not there are further guidelines for approval and use, or whether case-by-case decisions will be rendered based on some defined criteria.

Applicability: Issue-specific policies will 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 foreign software is intended to apply only to the organization's own onsite resources and employees and is not to be applicable to contractor organizations 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: Also included in issue-specific policies should be the assignment of roles and responsibilities. This would mean, to continue with the above example, that if the policy permits foreign 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. Likewise, it would need to be clarified who would be responsible for ensuring that only approved foreign software is used on organizational IT resources and, perhaps, for monitoring users in regard to foreign software.

Related to the assignment of roles and responsibilities is the inclusion of guidelines for procedures and enforcement. The issue-specific policy on foreign-software, for example, might include procedural guidelines for checking disks used by employees at home or at other locations. It might also state what the penalties would be for using unapproved foreign software on the organization's IT systems.

Points of Contact: For any issue-specific policy, the appropriate individuals in the organization to contact for further information, guidance, and enforcement should be indicated. 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, or system administrator. For yet other issues, the point-of-contact might be a 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 his/her immediate superior, a system administrator, or a computer security official.

Areas Appropriate for Issue-specific Policies

Some of the areas in which management today needs to consider issue-specific IT security policies are covered in this section. These topics are intended to provide examples and serve as sources for ideas and analysis. Although many of these topics are standard to any discussion of IT security, an organization would necessarily need to tailor its policies relating to them to meet its own unique needs.

Physical security: The physical protection of and access to IT resources and facilities will generally need to be addressed in one or more specific policies. In organizations with extensive IT systems and equipment, this may mean developing policies that address such issues as who has access to what sites/locations; how often risks to installations are be analyzed and by whom; what types of physical access controls and monitoring equipment are put in place; what responsibilities will be assigned to trained security officials and what activities and responsibilities will be required of all employees.

Personnel Security: Depending on the types of activities being performed, degree of data sensitivity to be encountered, and sheer numbers of personnel, specific security policies related to personnel screening, requirements, hiring, training, evaluating, and firing may need to be developed and administered. It may be appropriate that a trained personnel security specialist initiate, review, approve, and perform all security-related personnel actions.

Communications Security: Communications security is a complex technical specialty unto itself. In organizations where day-to-day business relies on communicating routinely with remote locations, the security of the communications transmissions and lines is usually an issue that needs to be addressed by policy. If the data being transmitted is highly sensitive, then this concern is magnified, and issue-specific security policies may need to be developed on a number of activities. Issues associated with the use of cryptography and its related options and procedures (discussed in Chapter 19), the use of modems and dial-in lines, and precautions against wiretapping are just some of the potential issues to be addressed. Additionally, as noted earlier, the proliferation of E-mail has introduced many security- and privacy-related issues for which organizations need to document positions and policies.

Administrative Security: Administrative security as it applies to IT system management and oversight activities comprises many potential security policy issues. Included are such topics as input/output controls, training and awareness, security certification/accreditation, incident reporting, system configurations and change controls, and system documentation.

Risk Management: Risk management involves assessing IT resources in terms of potential threats and vulnerabilities and planning the means for counteracting those identified risks. Issues that will need to be addressed by policies include how, by whom, and when the assessments should be performed; and what type of documentation should result.

Contingency Planning: Related to Risk Management, Contingency Planning means planning for the emergency actions to be taken in the event of damage, failure, and/or other disabling events that could occur to systems. Issues that need to be addressed by policies include determining which systems are most critical and therefore of highest priority in contingency planning; how the plans will be tested, how often, and by whom; and who will be responsible for approving the plans.

Policy Implementation

Policy implementation is a process. Policy cannot merely be pronounced by upper management in a one-time statement or directive with high expectations of its being readily accepted and acted upon. Rather, just as formulating and drafting policy involves a process, implementation similarly involves a process, which begins with the formal issuance of policy.

Policy Visibility

Especially high visibility should be afforded the formal issuance of IT security policy. This is due to a combination of factors, including the following:

- · · Nearly all employees at all levels will in some way be affected;
- · · Major organizational resources are being addressed;
- · · Many new terms, procedures, and activities will be introduced.

Providing visibility through such avenues as management presentations, panel discussions, guest speakers, question/answer forums, and newsletters can be beneficial, as resources permit. Including IT security as a regular topic at staff meetings at all levels of the organization can also be a helpful tactic. As an aspect of providing visibility for IT security policies, information should also be included regarding the applicable higher level directives and requirements to which the organization is responding. Educating employees as to the requirements specified by the Computer Security Act and related OMB circulars will help emphasize the significance and timeliness of computer security, and it will help provide a rational basis for the introduction of IT security policies.

Policy Documentation

Once IT security policy has been approved and issued, it may be initially publicized through memorandums, presentations, staff meetings, or a variety of means. As soon as possible, though, it will also need to be incorporated into formal policy documentation as well. The process of documenting policies will usually require updating existing documentation as well as creating new documentation.

Existing Documentation: IT security will need to be integrated into many existing activities and practices throughout many levels of the organization. This integration will be facilitated by revising any existing applicable documentation to reflect new procedures, rules, and requirements. Included may be the modification of various existing documents, forms, and plans at all levels of the organization to reflect the IT policy.

For example, if IT equipment purchases and/or upgrades have been reviewed and approved based on documented criteria such as cost, productivity, maintainability, etc., then security considerations may need to be introduced into that criteria. Also, if it has previously been the documented policy to review the progress and status of internal IT systems under development, then security-related concerns should be introduced into that review process.

New Documentation: Additionally, the development of many new documents, such as guidelines, standards, and procedures, may be required. This is often true in large organizations performing many different activities and having many levels of management. In such environments, different functional elements may have widely differing IT systems and needs to accommodate. It is therefore generally more practical, to the extent possible, to allow elements to tailor their implementations of policy to meet their unique needs. This can be accomplished through the development of documents containing more detailed procedures and practices to be used for specific kinds of systems and activities within functional elements.

For example, organizations will want to issue policies to decrease the likelihood of data loss due to technology failures and/or operator errors. A program-level policy might state something to the effect that: "It is the policy of the organization to ensure against data loss due to accidents or mishaps." In an area where extensive writing and editing of lengthy documents is performed, such as a word processing or technical publications unit, security documentation might be developed on saving work in-progress much more often than would usually be done, and/or utilizing automatic "save" features on IT systems and software. In a different type of functional area, however, where, for example, databases are maintained that do not undergo significant changes very often, the security documentation might focus on procedures for the database administrator to use in performing periodic (daily, weekly, etc.) backups of the system.

Appropriate visibility should be afforded the IT security policy through all applicable documentation. The more integral security policy is to all other aspects of daily routines, the more quickly the associated actions and practices will become natural to doing business. Ultimately, among the goals of policy are the assimilation of a common body of knowledge and values and the demonstration of appropriate corresponding behaviors. Those goals will be expedited by making the IT security policy integral to the organization through all avenues.

Cost Considerations

There are a number of potential costs associated with developing and implementing IT security policies. In some environments, the major costs may be those incurred through the numerous administrative and management activities required for drafting, reviewing, disseminating, and publicizing the policies. In some organizations, though, successful policy implementation may require additional staffing, training, and equipment. In general, how costly IT security policy development and implementation are to an organization will depend upon how much change needs to be accomplished in order to ensure adequate security and a basic standardization throughout the organization.

Interrelationships

IT security policy can be related to nearly every topic covered in this handbook on some level. This is because all of the topics discussed in the handbook have associated issues that organizations may need to address via policies. The topics most directly related, however, are: IT security program management and administration; risk management; personnel; security training and awareness; contingency planning; and physical and environmental security.

Conclusion

Formulating viable IT 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 both program-level and issue-specific policy components, a coherent set of policies - integrated into sensible practices and procedures - can be developed 6.1, para 2: IT security policy helps to provide basic standards, guidelines, and rules for everyone in an organization.

6.2, para 1: Program-level IT security policy establishes the security program and assigns program management responsibilities.

6.2.1.1, para 4: Program-level policy should be sufficiently broad in scope to include all of the organization's IT resources.

6.2.1.1, para 5: Program-level IT security policy goals should stress the universal concepts of integrity, availability, and confidentiality.

6.2.2, para 1: Issue-specific policies address particular activities, concerns, and, sometimes, systems.

6.2.2, para 4: New products, developments, and trends often require the creation of corresponding issue-specific policies.

6.2.2.2, para 1: Many activities within an organization should be considered when developing issue-specific policies, including physical security, personnel, communications, administrative security, risk management, and contingency planning.

6.3.1, para 1: IT security policy should be given especially high visibility in order to help ensure employee awareness and understanding.

6.3.2, para 4: Many existing documents of an organization will need to be revised to reflect IT security policies, and new documents may also need to be developed.