

IMPROVING INFORMATION SECURITY THROUGH POLICY IMPLEMENTATION

Herbert J. Mattord, CISSP

Kennesaw State University, Kennesaw GA
hmattord@kennesaw.edu

Michael E. Whitman, Ph.D., CISSP

Kennesaw State University, Kennesaw GA
mwhitman@kennesaw.edu

Abstract

Information security policy is essential to the success of any information security program because it is the primary process used by organizations to influence the performance of personnel in ways that enhance the information security of the organization's information assets. Whereas computer security can be thought of as the processes and techniques of securing IT hardware, software and data (including networks), information security is a broader concept. The processes of information security are concerned with the protection of the confidentiality, integrity and availability of information within systems comprising hardware, software, networks, data, procedures and personnel.

As organizations change through evolution of practices and hiring of new personnel for growth or replacement policy emerges as the mechanism whereby an organization defines what is to be secured and establishes what to secure, why it needs to be secured and perhaps how to achieve the desired levels of security.. Without sound policy as a foundation an organization is less likely to be successful in its mission to protect information assets.

Introduction

The success of any information security program lies in policy development. The lack of success in any particular program can often be attributed to failing to meet this need. The National Institute of Standards and Technology addressed this point in Special Publication SP 500-169 - *Executive Guide to the Protection of Information Resources*:

“The success of an information resources protection program depends on the policy generated, and on the attitude of management toward securing information on automated systems. You, the policy maker, set the tone and the emphasis on how important a role information security will have within your agency. Your primary responsibility is to set the information resource security policy for the organization with the objectives of reduced risk, compliance with laws and regulations and assurance of operational continuity, information integrity, and confidentiality.”ⁱ

As further elaborated by Charles Cresson Wood, in his widely referenced book *Information Security Policies Made Easy*,

“The centrality of information security policies to virtually everything that happens in the information security field is increasingly evident. [...] These policies will stipulate the type of [...] services that should be permitted, how to authenticate the identities of users, and how to log security-relevant events. An effective information security training and awareness effort cannot be initiated without writing information security policies because policies provide the essential content that can be utilized in training and awareness material.”ⁱⁱ

Policy is essential because it is the primary process in most organizations that can drive the performance of personnel in ways that enhance the information security of an organization's information assets.

Although information security policies are the least expensive means of information security control to execute, they are often the most difficult to implement. Policy controls typically cost only the time and effort the management teams spends to create, approve, and communicate them, and that employees spend integrating the policies into their daily activities. Even

when the management team hires an outside consultant to assist in the development of policy, the costs are minimal compared to the other forms of control, especially technical controls.

Policy, Standards, and Practices

Policy is “a plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters”ⁱⁱⁱ. In other words, policies are a set of rules that dictates acceptable and unacceptable behavior within an organization. Policies must also specify the penalties for unacceptable behavior, and define an appeal process. An example of a policy would be an organization’s prohibiting the viewing of pornographic Web sites at the workplace. To execute this policy, the organization must implement a set of standards. A **standard** is a more detailed statement of what must be done to comply with policy. In the implementation of the anti-pornography policy, the organization may create a standard that the network will block access to pornographic Web sites. **Practices, procedures and guidelines** explain how employees will comply with policy.

For policies to be effective they must be properly disseminated, via printed personnel manuals, organizational intranets, and periodic supplements. All members of the organization must read, understand, and agree to abide by the organization’s policies. Policies require constant modification and maintenance. As the needs of the organization evolve, so must its policies.

Some basic rules must be followed when shaping any policy, including information security policy:

- Policy should never conflict with law
- Policy must be able to stand up in court, if challenged
- Policy must be properly supported and administered

Since policy is often difficult to implement, Bergeron and Bérubé have proposed guidelines for the formulation of computer policy, which are also directly applicable to information security policy: “All policies must contribute to the success of the organization, management must ensure the adequate sharing of responsibility for proper use of information systems, and End users of information systems should be involved in the steps of policy formulation.”^{iv} Bergeron and Bérubé further note that while it is an admirable goal for policies to be complete and comprehensive, too many policies or policies that are too complex can lower end user satisfaction.^v

In order to produce a complete information security policy, management must define three types of information security policy. These three types are based on National Institute of Standards and Technology Special Publication 800-14vi, which outlines the requirements of writing policy for senior managers.

The three types of policy are:

- Enterprise information security program policy
- Issue-specific information security policies
- Systems-specific information security policies

Enterprise Information Security Policy

An **enterprise information security policy (ESP)**—also known as a security program policy, general security policy, IT security policy, high-level information security policy or information security policy—sets the strategic direction, scope, and tone for all of an organization’s security efforts. The ESP assigns responsibilities for the various areas of information security, including maintenance of information security policies, and the practices and responsibilities of end users. In particular, the ESP guides the development, implementation, and management requirements of the information security program, which must be met by information security management, IT development, IT operations and other specific security functions.

This policy must directly support the vision and mission statements of the organization. It must also address legal compliance, typically in two areas:

“1) General compliance to ensure meeting the requirements to establish a program and the responsibilities assigned therein to various organizational components and 2) the use of specified penalties and disciplinary action.”^{vii}

The ESP is an executive-level document, drafted by the CISO in consultation with the CIO, is usually two to ten pages long, and shapes the security philosophy in the IT environment. The ESP usually does not require repeated or routine modification, unless there is a change in the strategic direction of the organization.

The ESP plays a number of vital roles, not the least of which is to state the importance of information security in support of the organization’s mission and objectives. Unless the ESP directly reflects this association, the policy will likely become confusing and counter-productive. Though specifics of ESPs vary from organization to organization, most ESP documents should provide the following:

- An overview of the corporate philosophy on security
- Information on the structure of the information security organization and individuals that fulfill the information security role
- Fully articulated responsibilities for security that are *shared by all members* of the organization (employees, contractors, consultants, partners and visitors)
- Fully articulated responsibilities for security that are *unique to each role* within the organization.

The components of a good ESP are shown in Table 1^{viii}:

Table 1 – Components of the ESP

Component	Description
Statement of Purpose	Answers the question “What is this policy for?” Provides a framework for the helps the reader to understand the intent of the document. Can include text such as: “This document will: Identify the elements of a good security policy, explain the need for information security. specify the various categories of information security, identify the information security responsibilities and roles, [and] identify appropriate levels of security through standards and guidelines This document establishes an overarching security policy and direction for our company. Individual departments are expected to establish standards, guidelines, and operating procedures that adhere to and reference this policy while addressing their specific and individual needs.” ^{ix}
Information Technology Security Elements	Defines information security. For example “Protecting the confidentiality integrity and availability of information while in processing, transmission and storage, through the use of policy, education & training, and technology...” It can also lay out security definitions or philosophies in order to clarify the policy.
Need for Information Technology Security	Provides information on the importance of information security in the organization and the obligation (legal and ethical) to protect critical information whether regarding customers, employees, or markets.
Information Technology Security Responsibilities and Roles	Defines the organizational structure designed to support information security within the organization. Includes identification of categories of individuals with responsibility for information security (IT dept, management, users) and their information security responsibilities, including maintenance of this document.
Reference to Other Information Technology Standards And Guidelines	Outlines lists of other standards that influence and are influenced by this policy document. These could include relevant laws, federal and state, as well as other policies in place in the organization.

The formulation of program policy in the ESP establishes the overall information security environment. As noted earlier, there are any number of specific issues that require policy guidance beyond what can be offered in the ESP. The next level of policy document, the issue-specific policy, delivers the specificity.

Issue-Specific Security Policy (ISSP)

A sound **issue-specific security policy** provides detailed, targeted guidance to instruct all members of the organization in the use of technology based systems. The ISSP should begin with an introduction of the fundamental technological philosophy of the organization. It should assure the member of the organization that the purpose of the policy is not to provide a legal foundation for persecution or prosecution, but to provide a common understanding of the purposes for which an employee can and cannot use the technology. Once this understanding is established, employees are free to use the technology without seeking approval for each type of use. This serves to protect both the employee and the organization from inefficiency and ambiguity.

An effective ISSP articulates the organization’s expectations about how the technology-based system in question should be used as well as documents how the technology-based system is controlled and identifies the processes and authorities that provide this control. When implemented, it can serve to indemnify the organization against liability for an employee’s inappropriate or illegal system use.

An effective ISSP is a binding agreement between parties (the organization and its members) and shows that the organization has made a good faith effort to ensure that its technology is not used in an inappropriate manner. Every organization’s ISSP will address specific technology-based systems and require frequent updates. It will also contains an issue statement on the organization’s position on an issue^x. An ISSP may be drafted to cover many topics, including electronic mail, use of the Internet and the World Wide Web, specific configurations of computers to defend against worms and viruses or one of many other topics.

The specific situation of any particular organization dictates the exact wording of the security procedures as well as issues not covered within these general guidelines, but each policy should include the following sections:

- Statement of Purpose
- Authorize Access and Usage of Equipment
- Prohibited Usage of Equipment
- Systems Management
- Violations of Policy
- Policy Review and Modification
- Limitations of Liability

There are a number of approaches for creating and managing ISSPs. Three of the most common are to create a number of independent ISSP documents, each tailored to a specific issue, or to create a single comprehensive ISSP document that aims to cover all issues, or to create a modular ISSP document that unifies policy creation and administration, while maintaining each specific issue’s requirements. Table 2 describes the advantages and disadvantages of each approach.

Table 2 ISSP Approaches

Approach	Advantages	Disadvantages
Individual Policy	Clear assignment to a responsible department Written by those with superior subject matter expertise for technology-specific systems	Typically yields a scattershot result that fails to cover all of the necessary issues Can suffer from poor policy dissemination, enforcement, and review
Comprehensive Policy	Well controlled by centrally managed procedures assuring complete topic coverage. often provides better formal procedures than when individually formulated, usually identifies processes for dissemination, enforcement, and review	May tend to over-generalize the issues and skip over vulnerabilities, may be written by those with less complete subject matter expertise
Modular Policy	Often considered an optimal balance between the individual ISSP and the comprehensive ISSP approaches, well	May be more expensive than other alternatives, implementation can be difficult to manage

	controlled by centrally managed procedures assuring complete topic coverage, clear assignment to a responsible department, written by those with superior subject matter expertise for technology-specific systems	
--	--	--

The recommended approach is the modular policy, which provides a balance between issue orientation and policy management. The policies created via this approach are individual modules, each created and updated by individuals responsible for a specific issue. These individuals report to a central policy administration group that incorporates these specific issues into an overall policy distribution mechanism.

Systems-Specific Policy (SysSP)

While issue-specific policies are formalized as written documents, distributed to users, and agreed to in writing, systems-specific policies (SysSPs) are frequently codified as standards and procedures used when configuring or maintaining systems. One example of a SysSP is a document describing the configuration and operation of a network firewall. This document could include a statement of managerial intent, guidance to network engineers on selecting, configuring, and operating firewalls, and an access control list that defines levels of access for each authorized user. Systems-specific policies can be organized into two general groups, management guidance and technical specifications.

Conclusion

The early years of the twenty-first century have seen the emergence of information security as both a practical area of specialization in Information technology and as an academic discipline in post-secondary education. As many new members join the information security community, it is important that the primary role of policy as the mechanism whereby an organization defines what is to be secured is clearly understood. Without sound policy as a foundation, policy constructed with the same care and attention to detail required by all parts of the information security mission, an organization is less likely to be successful in its mission to protect information assets.

References

ⁱ The National Institute of Standards and Technology, *Executive Guide to the Protection of Information Resources* retrieved November 12, 2003 from <http://csrc.nist.gov/publications/nistpubs/500-169/sp500-169.txt>

ⁱⁱ Charles Cresson Wood, *Information Security Policies Made Easy*, Ninth Edition (2003) NetIQ Corporation p 1.

ⁱⁱⁱ Merriam-Webster. "policy." *Merriam-Webster Online*. [Cited 24 June 2002]. Available from the World Wide Web <<http://www.m-w.com/cgi-bin/dictionary>>.

^{iv} Bergeron, F. and Bérubé, C. "End Users Talk Computer Policy." *Journal of Systems Management*. 41(12) December 1990. Pp. 14-17.

^v Ibid.

^{vi} The National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Securing Information Technology Systems* retrieved November 12, 2003 from <http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>

^{vii} The National Institute of Standards and Technology, *An Introduction to Computer Security: The NIST Handbook* retrieved November 12, 2003 from <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>.

^{viii} Derived from a number of sources, the most notable of which was retrieved November 12, 2003 from <http://www.wustl.edu/policies/infosecurity.html>

^{ix} Information Security Policy, Washington State University, retrieved November 12, 2003 from <http://www.wustl.edu/policies/infosecurity.html>

^x Ibid.