DATA SECURITY MANAGEMENT

THE SECURITY POLICY LIFE CYCLE: FUNCTIONS AND RESPONSIBILITIES

Patrick D. Howard, CISSP

INSIDE

Policy Functions; Policy Responsibilities; Policy Function–Responsibility Matrix

It is time to let out a great sigh of relief. After countless months of tedious effort, one has succeeded in writing one's company's Internet Usage Policy. Time to celebrate, right? Well, maybe. It is true that the greatest hurdle for many organizations is documenting its information security policies. This is a major accomplishment because of the importance of the task and the substantial effort normally involved in such an effort. The author does not want to spoil the party, but documenting one's policies in writing is only the beginning of the policy life cycle.

POLICY FUNCTIONS

Actually, there are eleven functions that must be performed throughout the life of policy documentation, from cradle to grave.

1. *Creation*. This first phase includes the actual planning for, research on, and creation of the policy. There also is the coordination of the research and writing with other organizations, both internal and external. This is the most obvious phase of the policy documentation life cycle because it normally requires the most persistent effort.
2. *Review*. This is the assessment of the policy by an independent individual or body prior to its final

PAYOFF IDEA

The life cycle of a security policy is much more complex than simply drafting written requirements and posting them on the corporate intranet. Employment of an organized policy life-cycle approach as described here will help an organization ensure that these interrelated functions are performed consistently through the assignment of responsibility for the execution of each according to level of policy. This approach can greatly improve the effectiveness of organizational security policies, which is always a major goal but is often a major shortcoming.

Auerbach Publications

approval. It entails identifying the individuals or groups responsible for the review, presenting the policy, addressing questions regarding the policy, explaining the policy's context, justifying the policy, addressing comments and recommendations for changes to the policy, and making necessary adjustments and revisions.

3. *Approval*. The approval phase is the endorsement of the policy by a company official in a position of authority, which permits the implementation of the policy. During this phase, the appropriate authority for approval must be identified, buy-in to the policy must be obtained, the appropriate authority for approval must be determined, and issues regarding interim or temporary approval must be considered.
4. *Communication*. Once the policy has been approved, it must be initially disseminated to company employees or contractors who are affected by the policy. Sub-tasks of this phase include making a determination of the extent of the initial distribution; addressing issues of geography, language, and culture; prevention of unauthorized disclosure if applicable; method of distribution; and use of the supervisory chain.
5. *Implementation*. This phase encompasses activities to initially execute the policy, such as ensuring that the policy is understood; interpreting how the policy can best be implemented in various situations and organizational elements; monitoring the pace, extent, and effectiveness of implementation activities; and measuring the policy's impact on operations.
6. *Awareness*. The awareness phase comprises continuing efforts to ensure that personnel are aware of the policy in order to facilitate their compliance with policy requirements. This is done by addressing various audiences within the organization (executives, line managers, users) with tailored awareness messages regarding the need for adherence to the policy.
7. *Exceptions*. Because of operational requirements, timing, personnel shortages, etc., not every policy can be complied with as intended. Therefore, exceptions to the policy will probably need to be granted. There must be a process to ensure that such requests are tracked, evaluated, submitted for approval/disapproval, documented, and monitored during the period of approved noncompliance.
8. *Compliance monitoring*. During the compliance monitoring phase, the effectiveness of efforts to implement the policy is tracked and reported. This information results from formal audits, inspections, and reviews; from supervisors and employees; and from violation reports and incident response activities. This phase includes activities to monitor the level of compliance with the policy and to report deficiencies to appropriate management authorities.
9. *Enforcement*. The compliance muscle behind the policy is effective enforcement. Acts or omissions that violate the policy must be ad-

dressed through management's enforcement efforts. This means that once a violation is identified, appropriate corrective action must be determined and applied to address the violation and to prevent its recurrence.

10. *Maintenance.* This phase addresses the process of ensuring the currency and integrity of the policy. Issues dealt with in this phase include tracking drivers for change (i.e., changes in technology, processes, people, organization, business focus, etc.), recommending and coordinating policy modifications as necessary, documenting change activities, and ensuring the availability of the policy. When changes to the policy are required, several phases must be revisited — review, approval, communication, and implementation in particular.
11. *Retirement.* After the policy has served its useful purpose (e.g., the company no longer uses the technology for which it applies, or it has been superseded by another policy), then it must be retired. This entails removing it from the inventory of active policies, archiving it for future reference, and documenting information about the decision to retire the policy (i.e., justification, authority, date, etc.).

These eleven distinct phases comprise the major functions that must be performed over the life cycle of a given policy. It is possible to combine certain functions. No matter how they are grouped, however, they need to be performed. In fact, several of the phases must be done iteratively. In particular, maintenance, awareness, compliance monitoring, and enforcement must be continuous over the life of the policy.

POLICY RESPONSIBILITIES

In many cases, the organization's information security (IS) function performs most of these functions and acts as the proponent for most policy documentation related to the protection of information assets. By design, the IS function exercises day-to-day responsibility for securing information resources and, as such, should "own" and exercise centralized control over security-related policies, standards, procedures, and guidelines. This is not to say, however, that the IS function and its staff will always be the proponent for a security policy. For example, system owners should have responsibility for establishing requirements necessary to implement higher organization policies for their own systems. While requirements such as these must comport with higher-level policy directives, they must be owned by the organizational element that has the largest stake in ensuring the effectiveness of the policy.

While the proponent for a policy exercises continuous responsibility for the policy over its entire life cycle, there are several factors that have a significant impact on the assignment of direct responsibility for performing specific policy functions in an organization.

The principle of separation of duties should be applied in determining responsibility for a particular policy function to ensure that checks and balances are applied. An official or group that is independent of the proponent should review the policy, and an official who is senior to the proponent should be charged with approving the policy. And, the audit function as an independent element should be tasked with monitoring compliance with the policy.

Additionally, for reasons of efficiency, organizational elements other than the proponent should be assigned responsibility for the policy. Communication of the policy is best carried out by the organizational element chartered with that function (i.e., knowledge management, corporate communications, etc.). The organization security function is normally charged with awareness efforts because it is often in the best position to make employees/contractors aware of the policy.

Also, limits on span of control that the proponent exercises come into play. The proponent can play only a limited role in compliance monitoring and enforcement of the policy because he or she cannot be in all places where the policy has been implemented at all times. Line managers are in a better position to assume responsibility for these functions and can provide the proponent assurance that the policy is being adhered to.

Because of his or her placement in the organization, the proponent may also be limited by a lack of knowledge of the environment in which the policy will be implemented. Employment of a policy review board can provide a broader understanding of business conditions that will be affected by the policy. Such a board can help ensure that the policy is written so as to promote its effective implementation and can be used to effectively assess situations where exceptions to the policy may be warranted.

Finally, the scope of the policy also affects the responsibility for policy life-cycle functions. How much of the organization is affected by the policy? Does it apply to a single business unit, all users of a particular technology, or the entire global enterprise? This distinction makes a very large difference.

POLICY FUNCTION–RESPONSIBILITY MATRIX

To ensure that all functions in the policy life cycle are addressed, organizations should establish a framework that facilitates ready understanding, promotes consistent application, establishes a hierarchy of lower policy levels that support higher levels in the structure, and effectively accommodates frequent technological and organizational change. Exhibit 1 provides a reference for assignment of responsibilities related to security policies by policy function.

For the purpose of this grid, generally accepted definitions are used. A "policy" is defined as a broad statement of principle that presents man-

EXHIBIT 1 — Policy Function-Responsibility

Function	Responsibility		
	Policies	**Standards**	**Procedures**
Creation	Organization security function	Organization security function	Proponent element
Review	Policy evaluation committee	Policy evaluation committee	Proponent management/ organization security function
Approval	Chief executive officer	Chief information officer	Department vice president
Dissemination	Communications department	Communications department	Proponent management
Implementation	Managers and employees organizationwide	Managers and employees organizationwide as applicable	Managers and employees within the proponent element
Awareness	Organization security function	Organization security function	Proponent management
Exception review/ approval	Policy evaluation committee	Policy evaluation committee	Department management
Compliance monitoring	Line managers/ organization security function/audit function	Line managers/ organization security function/audit function	Proponent element line managers/ organization security function/audit function
Enforcement	Line managers	Line managers	Proponent element line managers
Maintenance	Organization security function	Organization security function	Proponent element
Retirement	Organization security function	Organization security function	Proponent element

agement's position for a defined control area. A "standard" is defined as a rule that specifies use of a particular product in response to a given situation and is a mandatory directive for carrying out policies. "Procedures" define mandatory courses of action; specifically, step-by-step actions as to how policies and standards will be implemented in a given situation. An example of interrelated security requirements at each level might be an electronic mail security policy for the entire organization at the highest "policy" level. This would be supported by various standards; for example, one might be that e-mail messages be routinely encrypted using PGP. And, continuing the example, "procedures" would be specific requirements for how the e-mail security policy and its supporting standards are to be applied in a given business unit.

This model proposes that responsibilities for functions related to policies and standards be quite similar. The organization security function should be the proponent for most security-related policies and standards

(a good example of an exception to this is the Human Resources department serving as the proponent for employee hiring policies). The significant difference between the responsibilities for policies and standards is the level of approval required for each and the extent of the implementation. Policies are organizationwide requirements, whereas standards might only relate to a specific part of the organization. On the other hand, responsibilities for functions related to procedures are distinctly different from those for policies and standards. Exhibit 1 shows that proponency for procedures rests outside the organization security function and is decentralized based on their limited applicability by organizational element. Although procedures are created and implemented (among other functions) on a decentralized basis, they must be consistent with higher organization security policy and therefore should be reviewed by the organization security function. Additionally, the security and audit functions should provide feedback to the proponent on compliance with procedures when conducting reviews and audits.

SUMMARY

The life cycle of a security policy is much more complex than simply drafting written requirements and posting them on the corporate intranet. Employment of an organized policy life-cycle approach as described here will help an organization ensure that these interrelated functions are performed consistently through the assignment of responsibility for the execution of each according to level of policy. This approach can greatly improve the effectiveness of organizational security policies, which is always a major goal but is often a major shortcoming.

Patrick D. Howard, CISSP, was manager of Methods and Administration, Global Security Practice, for Netigy Corporation.

Auerbach Publications