InfoSec Policy – The Basis for Effective Security Programs

Herbert J. Mattord
Kennesaw State University, USA

Michael E. Whitman
Kennesaw State University, USA

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 this unmet need to build the foundation for success. In 1989, the National Institute of Standards and Technology addressed this point in *Special Publication SP 500-169: Executive Guide to the Protection of Information Resources* (1989):

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 (p.1).

Policy is the essential foundation of an effective information security program. As stated here by Charles Cresson Wood, in his widely referenced book *Information Security Policies Made Easy* (2003),

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 (p.1).

Policy is essential because it is the primary mechanism an organization possesses to inform and enforce expected behaviors in employees. Policy has the effect of law within the confines of the institutions. However, while *ignorantia legis neminem excusat* (ignorance of the law is no excuse) is prevalent in the public domain, ignorance of policy is legally defensible.

Although information security policies are among the least expensive information security controls to create, they are often the most difficult to implement. Policy-based controls typically cost only the time and effort the management teams spends to create, approve, and communicate them, and the time and effort 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 (Whitman & Mattord, 2004).

BACKGROUND

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" (Merriam-Webster, 2002). In other words, policies are a set of rules that dictate 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 (i.e., procedures and guidelines) explain how employees will comply with policy.

For policies to be effective they must be properly disseminated, via personnel manuals, organizational intranets, periodic supplements, staff meetings and/or training (to name a few). All members of the organization must read, understand, and agree to abide by the organization's policies. Failure to ensure each of these

requirements can negate the regulatory effect of policy. 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 (1990) have proposed guidelines for the formulation of computer policy, which are also directly applicable to information security policy:

1. "All policies must contribute to the success of the organization.
2. Management must ensure the adequate sharing of responsibility for proper use of information systems.
3. End users of information systems should be involved in the steps of policy formulation" (p. 16).

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.

As is evidenced in Figure 1, in order to secure information an organization must place protection mechanisms at multiple points. This is easily done in the electronic arena, where most threats come through the Internet, to the internal network, to the systems that house information, and finally to the information itself. However, inside an organization you may only have a few opportunities to protect information from those that use it. These opportunities include security education, training and awareness programs (SETA) and policy.

The use of multiple layers of protection is a concept called defense-in-depth, whereby security components at multiple layers serve to back each other up in the event that one layer's controls fail. Until sound and useable IT and information security policy is developed, communicated, and enforced, no additional resources should be spent on controls other than policy.

EFFECTIVE INFORMATION SECURITY POLICIES

To produce complete information security policy in the organization, management must use three types of information security policies. These three types are based on National Institute of Standards and Technology Special Publication 800-14 (1996), which outlines the requirements of writing policy for senior managers. This document is recommended for professionals involved in creat-

Figure 1. Spheres of use and protection of information (Whitman & Mattord, 2003)