SANS Institute
Information Security Reading Room

Developing Effective Information Systems Security Policies

Daniel Lee

Copyright SANS Institute 2019. Author Retains Full Rights.

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Full Name: R. Daniel Lee
Course/Certification: GSEC
Version: v1.2f
Status: Resubmission
Group: Baltimore Conference

DEVELOPING EFFECTIVE INFORMATION SYSTEMS SECURITY POLICIES

ABSTRACT

This paper takes a top-down approach and provides a high-level overview for developing effective information systems policies. The opening section describes the importance of management commitment. A management oversight committee is introduced as the primary team representing an organization for the purposes of implementing an information systems security program based on policy. A general outline for designing an effective information systems security policy is then proposed. Finally, the conditions necessary for effective policies are described.

INTRODUCTION

Information systems security policies primarily address threats. In the absence of threats, policies would be unnecessary—one could do as one chooses with information. Unfortunately, threats do exist and information systems security policies are necessary to provide a framework for selecting and implementing countermeasures against them. An enforceable written policy helps ensure that everyone within the organization coherently behaves in an acceptable manner with respect to information security.

A well-designed information security policy defines the objectives of the information system of an organization and outlines a strategy to achieve these stated objectives. Conversely, an information system without security policies is likely to be a disjoint collection of countermeasures that address a variety of threats [10]. Information systems security policies, then, can often be used to help integrate the many different aspects of an enterprise to achieve business objectives.

Policies, standards, guidelines, and training materials that are obsolete and not enforced are particularly dangerous to an organization because management is often deceived into believing that security policies do not exist and that the organization is operating more effectively than it actually is. All organizations need to periodically review, test, and discard un-enforced and otherwise obsolete rules, controls, and procedures to avoid this false sense of security. An alternative to periodic reviews is to specify a time limit for applying policies and standards and

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

assign limited life span to mandatory controls, specifying when they should become effective and when they should be nullified or replaced—a technique generally referred to as sunsetting.

Computers are inherently vulnerable to a wide array of threats. It is generally worse to have no safeguards at all than to think that security is in place when it is not. This situation, known as negative value security, fosters complacency and diverts attention from the information assets, which are mistakenly presumed to be secure, making the information more attractive to hackers or more vulnerable to accidental loss. Information systems security policies are designed to address these threats.

MANAGEMENT COMMITMENT

Management commitment to security is essential to motivate information resource owners and users and to provide the visibility needed by the information systems security team to ensure the support of the business units. Because there are few natural motivations for security, other than actual loss experience, managerial commitment to information systems security is probably the most important factor in a successful security system. In a distributed computing environment, this commitment can be demonstrated to end-users and systems staff through the managers' own practices and performance reviews. Security training materials, guidelines, and computing practices should be signed off and approved by the authoritative local sources—typically managers who decide and issue rewards and penalties.

In an interview with Bob Artner of TechRepublic, William Malik, Vice President and Research Area Director for the Gartner Group, states that senior management has to recognize that the integrity of the enterprise depends on their commitment to information security and set the example for the organization [1]. It is important to note that management commitment does not guarantee success, but its absence will certainly increase the likelihood of failure.

Management support of security provides the information systems security team with high visibility and fosters good rapport with high-level managers, particularly the senior managers of information intensive business units. Without the support of those individuals for the information systems security effort, their employees are less likely to support the effort. The best time to obtain visibility for information security is when a loss occurs. If the loss occurs in the organization or business unit with the most resistance to information systems security or the greatest need for security, then the need for information systems security becomes more apparent. Emphasizing the negative effects of a loss experience on the whole organization can be one way of applying pressure to motivate all business units to improve security.

Another way to obtain visibility is for the information systems security team to publish lists of business units ranked by the quality of their information security. This offers a positive reinforcement for the business units that take an active role in information systems security and applies pressure to those business units that do not.

MANAGEMENT OVERSIGHT COMMITTEE

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Many organizations have a management oversight committee for information systems security. Others organizations include information systems security issues in general oversight committees for technical or administrative concerns. In either case, the constituency of the oversight committee often reflects central IT services or corporate security, but does not specifically apply to information systems security for a distributed computing environment. In this case, the organization may need to reorganize or expand the existing committees to represent the new order of distributed computing needs. Members should include the senior managers of business units actively engaged in the distributed computing environment, as well as managers who rely on external data communications, such as field sales and services. This type of committee, which is crucial for ensuring ongoing managerial commitment, should be responsible for authorizing, reviewing, approving, and distributing corporate policies and standards. To increase the effectiveness of this committee, at least one member should have regular access to the senior managers of the organization.

POLICY DEVELOPMENT RESPONSIBILITIES

Either the information systems security team or the IT policies and standards group under the direction of the information systems security team should be responsible for drafting appropriate policies and policy updates. As an alternative, some organizations assign the responsibility to a task group under the auspices of a management oversight committee. This is a common arrangement when the policies are being written or updated in conjunction with a reorganization or more drastic re-engineering of the information systems security team. It is generally not a good idea to assign the policy-writing task to third-party consultants or use shelfware since the style and form should be consistent with existing policies and should reflect the corporate culture [3,5].

It is important that the team drafting information systems security policies be sufficiently familiar with both current technologies and corporate culture to make intelligent decisions. Familiarity with current technologies requires an understanding of both the security capabilities and the limitations of technological solutions to protect the organization against threats. Understanding the corporate culture additionally allows the policy development team to design an information systems security policy that can best ensure compliance.

Prior to drafting new polices, it is often helpful to review policies of similar organizations to use as models. Although Mike Cunningham and Raymond Iandolo independently offer examples of acceptable use policies for review in the SANS Reading Room, Charles Cresson Wood and the SANS Institute offer a more comprehensive collection of policies that an organization can be tailored for its use [2,4,9,11].

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

TYPES OF POLICIES

Establishing policy is very much an issue of corporate culture. Management support, wording, and distribution depend upon history, loss experience, the business and industry, government regulations, the personal philosophies of senior management, previous policies, and other factors within the organization [2,6,7,8,11]. If the corporate culture supports specific written policies on various subjects such as IT, various internal services, and ethics, then it is likely that a written policy on information systems security will exist. However, some organizations have a policy of not having written policies. Attorneys often do not like policies because they can be used against the organization if it violates them, and policies are often violated as a means to achieve short-term objectives for resolving business problems or achieving business goals.

If an organization distributes a written policy, it should be mandatory and reflect senior management's requirements for organizational behavior. When policies are written at a sufficiently high level of abstraction, they do not need to be changed as the IT department and organization change. Organizational changes such as mergers, acquisitions, reengineering, or the adoption of an industry standard can occur with little or no need to modify the policies. Information systems security policies should be flexible and should permit exceptions, when appropriate.

At the highest level of abstraction, policies are only a few pages long, with an officer or senior manager of the organization usually signing off on the policy to give it the proper authority. Some organizations include operational or tactical requirements in the form of control objectives with their policy statements. Others combine brief, high-level policy statements with more detailed standards, resulting in a document that may create problems when the organization needs disclose policies without revealing its standards. Therefore, it is generally a good practice to separate high-level policy from specific standards.

Operational or tactical policies are typically longer than high-level policy statements and may be either system-specific or issue-specific. Typically, middle managers, or higher, sign off on these documents.

POLICY ACCEPTANCE

User awareness, education, and participation are key factors toward gaining policy acceptance. These factors can be promoted through information systems security marketing. The objective of security marketing is to inform, educate, and persuade the business units and users to engage in the secure computing practices outlined by policy, including providing process improvement suggestions to the management oversight committee [3,7,10].

In reality, neither external nor internal threats necessarily lead toward compliance. So it is essential that the security marketing team effectively convey the roles and responsibilities of the business units and users with respect to information systems security. Business units and users must understand that seemingly innocent computing behavior can have catastrophic effects.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Business units and users must also realize that information systems security policies are not infallible and unchangeable directives arbitrarily developed by an obscure and remote security policy development team. Business units must know that they have access to the policy development team so that they work together and improve existing policies. In this manner, policies can evolve toward achieving a balance between information systems security and business practices that can allow the organization to optimally reach its business objectives.

Since no policy can address every situation that might potentially arise in the future, it is important that there be a widespread realization of the underlying principles of the organization's information systems security policies. This knowledge can serve as a guide in the undefined areas that stretch existing boundaries not originally envisioned by the policy development team.

The challenge with corporate information systems security policies is that they need to be understood and practical in order to be effective. Policy acceptance is dependent on the policy's inherent ability to describe acceptable and/or unacceptable behavior with respect to information systems security. The policy should outline who is responsible for what (implementation, enforcement, audit, and review), what the basic information systems security policies are, and the reasons for the policies. Arbitrary policies with no explanation are likely to be ignored. A clear, concise, coherent, and consistent policy that sets user information handling expectations is more likely to be followed.

Finally, the security marketing team needs to make the information systems security policies easily accessible to the business units and users. It is advantageous for organizations to automate the process of disseminating the information contained in its security policies in order to educate its user community. Policies that have traditionally been presented in a linearly printed format often fail to consider the reader's existing knowledge, forcing even the most savvy users to seemingly research volumes of basic security information. However, familiar hypertext technology is one solution that can facilitate the education of users about an organization's information systems security policies. In an environment where users can control their own learning experience, the flexibility that hypertext technology provides is often more conducive for learning since the program can be individually tailored for each user.

IMPORTANCE OF POLICY

Information systems security policies are designed to inform the members of an organization of their obligatory responsibilities for protecting the information systems of their organization. These policies often specify the mechanisms through which these responsibilities can be performed. Information systems security policies also provide baselines to acquire, configure, and audit information systems for compliance with the policy. Information systems security tools in the absence of policy, then, are of limited usefulness [6].

Policies are significantly more important in a distributed computing environment than a centralized computing environment because of the increased challenge of constraining activity from a remote location. Such policies must also be complete and clearly stated to reduce the amount of explanation and instruction that the organization needs to undertake to be certain they

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

are understood. Policies should include general descriptions and identifiers for business units and functions rather than the names of individuals so that they can transcend organization changes. They should be confined to general concepts rather than specific controls. For example, a policy stating, “Each computer user must be authenticated by an acceptable method” is better than the more specific policy stating, “Each computer user must be authenticated by a six-character password” since the policy does not need to be changed should strong authentication tokens replace passwords

Policy is also important in distributed computing environments as a means of establishing security discipline for a large, disparate group of users and business units that are generally only reached by formal communications and audit. This is particularly important when the organization relies heavily on contract or temporary personnel. Policies should reflect the accepted practices of an organization yet take advantage of all practical methods for influencing behavior and disseminating information within the distributed computing environment.

CONCLUSION

The process of developing an effective information systems security policy is straightforward. Shaped by threats to an information system, the information systems security policy defines the objectives of the information system of an organization and outlines a strategy to achieve these stated objectives. It is important that senior management is committed to upporting the information security initiative. A policy-writing team, commissioned by a management oversight committee, should construct the policy to reflect the corporate culture. Finally, a security marketing team needs to inform and educate the organization about its security policies and persuade the users to engage in secure computing practices. Business units and users must know that they are an integral part of the information systems security process. Although straightforward, this process is not easily executed and the information systems security team must constantly strive to improve the process and provide the best defense against threats to the organization.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

REFERENCES

[1] Artner, Bob. "Does Your Company Culture Value Corporate Security?" TechRepublic, 2000. http://www.techrepublic.com/article.jhtml?src=search&id=r00520001009ggp05.htm

[2] Crabb-Guel, Michele. "Building An Effective Security Infrastructure." SANS Institute Resources. http://www.sans.org/newlook/resources/policies/policies.htm

[3] Crume, Jeff. *Inside Internet Security: What Hackers Don't Want You to Know*. Pearson Education Limited, 2000.

[4] Cunningham, Mike. "Acceptable Use Policy." SANS Institute, 2001. http://www.sans.org/infosecFAQ/policy/use_policy.htm

[5] Desilets, Gary. "Shelfware: How to Avoid Writing Security Policy and Documentation that Doesn't Work." SANS Institute, 2001. http://www.sans.org/infosecFAQ/policy/shelfware.htm

[6] Fraser, Barbara, Editor. "Site Security Handbook," FYI 8, RFC 2196 September 1997. http://www.faqs.org/rfcs/rfc2196.html

[7] Fried, Stephen. "Information Security: The Big Picture – Part IV." SANS Institute, 2001.

[8] Guttman, Barbara and Bagwell, Robert. *Internet Security Policy: A Technical Guide*, National Institute of Standards and Technology, 1997. http://csrc.nist.gov/isptg/html/ISPTG.html

[9] Iandolo, Raymond. "Acceptable Use Policy Document." SANS Institute, 2001. http://www.sans.org/infosecFAQ/policy/accept_use.htm

[10] Schneier, Bruce. *Secret and Lies: Digital Security in a Networked World.* Wiley Computer Publishing, 2000.

[11] Wood, Charles Cresson. *Information Security Policies Made Easy, Version 7.* Baseline Software, Inc., 1999.

[12] Woodard, Everett. "Network Security: Policies & Procedures," Technical Support, Vol. **8** (11), 2000. http://www.naspa.com/PDF/2000/1100 TS PDFs/T0011007.pdf

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: October 17th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

Purple Team Summit & Training 2019	**Las Colinas, TXUS**	**Oct 21, 2019 - Oct 28, 2019**	**Live Event**
SANS Santa Monica 2019	**Santa Monica, CAUS**	**Oct 21, 2019 - Oct 26, 2019**	**Live Event**
SANS Training at Wild West Hackin Fest	**Deadwood, SDUS**	**Oct 22, 2019 - Oct 23, 2019**	**Live Event**
SANS Houston 2019	**Houston, TXUS**	**Oct 28, 2019 - Nov 02, 2019**	**Live Event**
SANS Orlando 2019	**Orlando, FLUS**	**Oct 28, 2019 - Nov 02, 2019**	**Live Event**
SANS Amsterdam October 2019	**Amsterdam, NL**	**Oct 28, 2019 - Nov 02, 2019**	**Live Event**
SANS Mumbai 2019	**Mumbai, IN**	**Nov 04, 2019 - Nov 09, 2019**	**Live Event**
Cloud & DevOps Security Summit & Training 2019	**Denver, COUS**	**Nov 04, 2019 - Nov 11, 2019**	**Live Event**
SANS DFIRCON 2019	**Coral Gables, FLUS**	**Nov 04, 2019 - Nov 09, 2019**	**Live Event**
SANS Paris November 2019	**Paris, FR**	**Nov 04, 2019 - Nov 09, 2019**	**Live Event**
SANS Sydney 2019	**Sydney, AU**	**Nov 04, 2019 - Nov 23, 2019**	**Live Event**
SANS London November 2019	**London, GB**	**Nov 11, 2019 - Nov 16, 2019**	**Live Event**
MGT521 Beta One 2019	**Crystal City, VAUS**	**Nov 12, 2019 - Nov 13, 2019**	**Live Event**
GridEx V 2019	**Online,**	**Nov 13, 2019 - Nov 14, 2019**	**Live Event**
SANS Gulf Region 2019	**Dubai, AE**	**Nov 16, 2019 - Nov 28, 2019**	**Live Event**
European Security Awareness Summit 2019	**London, GB**	**Nov 18, 2019 - Nov 21, 2019**	**Live Event**
SANS November Singapore 2019	**Singapore, SG**	**Nov 18, 2019 - Nov 23, 2019**	**Live Event**
Pen Test HackFest Summit & Training 2019	**Bethesda, MDUS**	**Nov 18, 2019 - Nov 25, 2019**	**Live Event**
SANS Austin 2019	**Austin, TXUS**	**Nov 18, 2019 - Nov 23, 2019**	**Live Event**
SANS Atlanta Fall 2019	**Atlanta, GAUS**	**Nov 18, 2019 - Nov 23, 2019**	**Live Event**
SANS Munich November 2019	**Munich, DE**	**Nov 18, 2019 - Nov 23, 2019**	**Live Event**
SANS SEC401 Madrid November 2019 (in Spanish)	**Madrid, ES**	**Nov 18, 2019 - Nov 23, 2019**	**Live Event**
SANS Cyber Threat Summit 2019	**London, GB**	**Nov 25, 2019 - Nov 26, 2019**	**Live Event**
SANS Tokyo November 2019	**Tokyo, JP**	**Nov 25, 2019 - Nov 30, 2019**	**Live Event**
SANS Bangalore 2019	**Bangalore, IN**	**Nov 25, 2019 - Nov 30, 2019**	**Live Event**
SANS Paris December 2019	**Paris, FR**	**Dec 02, 2019 - Dec 07, 2019**	**Live Event**
SANS Nashville 2019	**Nashville, TNUS**	**Dec 02, 2019 - Dec 07, 2019**	**Live Event**
SANS Security Operations London 2019	**London, GB**	**Dec 02, 2019 - Dec 07, 2019**	**Live Event**
SANS San Francisco Winter 2019	**San Francisco, CAUS**	**Dec 02, 2019 - Dec 07, 2019**	**Live Event**
SANS Frankfurt December 2019	**Frankfurt, DE**	**Dec 09, 2019 - Dec 14, 2019**	**Live Event**
SANS Cyber Defense Initiative 2019	**Washington, DCUS**	**Dec 10, 2019 - Dec 17, 2019**	**Live Event**
SANS Austin Winter 2020	**Austin, TXUS**	**Jan 06, 2020 - Jan 11, 2020**	**Live Event**
SANS Cairo October 2019	**OnlineEG**	**Oct 19, 2019 - Oct 24, 2019**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**