GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Corporate Information Security Program

Kathleen M. Seubert
GSEC Practical Assignment
Version V1.4b Option 1

February 3, 2003

Introduction

This paper will describe the components of a Corporate Information Security Program: Security Policies, Security Procedures and Awareness & Training. It will discuss the need for and the importance of security policies. It will touch upon creating and implementing security policies along with monitoring compliance with the policies. It will also discuss the importance of security policy awareness & training and finally policy maintenance.

It is my hope that the reader will understand the important role information and information technology occupies in today's environment and that a Corporate Information Security Program is needed to maintain the integrity, confidentiality and availability of these resources.

What is a Corporate Information Security Program?

A Corporate Information Security Program is comprised of three components:

- Security Policies – Documents designed to provide guidance on how to protect an organization's information and information systems.
- Security Procedures – Documents detailing the steps needed to accomplish a task.
- Awareness and Training – A necessary evil to get the message out.

What is a security policy?

"In basic terms, a security policy is a plan that defines "acceptable use" (based upon the acceptable risk) of all electronic media within a company or organization."(Jarmon) A security policy should detail how to both prevent and respond to threats to an organization's information - threats including but not limited to unauthorized access, modification, misuse and loss. It should also define the roles of all employees and the ramifications of non-compliance.

A security policy is not a manual; it is a high-level directive from executive management. "Infosecurity policies are statements of your organization's

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

approach to keeping its information safe. Policies don't specify how to get something done; they simply dictate that a goal be accomplished."(Berg)

Importance of and the need for a security policy

Before you can write a policy you need to understand what asset(s) you are trying to protect. "Your first priority is to develop a way to quantify and evaluate risk. You need to know what you are protecting and how much it's worth before you can decide how to protect it."(Berg)

Information systems and the information they contain are vital to an organization. "A security policy is needed to inform users and staff members of the need and their responsibility to protect the organization's technology and critical information."(Jarmon) A security policy should be based on preserving the availability, confidentiality and integrity of an organization's information resources and it should provide guidance on how to protect the information and information systems.

- Availability – The information system must be online and the information contained must be readily available. The user of the information system needs to know that the information can always be accessed.
- Integrity - The information contained in an information system must be protected from unauthorized or unintentional modification. The user must have confidence in the system and know that the information is current, accurate and has not been tampered with.
- Confidentiality - The information contained in an information system requires protection from unauthorized disclosure. The users of confidential information need to know that those accessing the data have been approved and "have a need know".

Creating the policy

"Do not reinvent the wheel! If policies are in place, review them and make necessary changes before starting from scratch. Identify and locate all assets. A security policy should be designed around the critical ones (assets) that are identified. An important next step is to identify threats to company assets. Identify which threats are critical and which ones are acceptable to the company."(Jarmon)

There has been some discussion on what type of policy to implement – one large umbrella policy or smaller, issue specific policies. I feel it would be easier to create and maintain smaller, issue specific policies. Regardless of the approach chosen, the same basic template should be used – this will give the policies a uniform look and feel.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Suggestions for issue specific polices are - but not limited to:

- Acceptable Use
- Email
- Password
- Anti Virus
- Privacy
- Internet Security
- Back-up
- Disaster Recovery
- Information Classification
- Mobile Computing (PDAs and Laptops)

Below is a suggested template along with a brief explanation for each section.

Title

This section occupies the first half of the first page and has the following headings:

- **Organizational Area:** Describes the area of the organization this policy applies to (enterprise wide, division, department, etc.).
- **Policy Name:** The name of the policy
- **Approval Date:** The date the policy was approved
- **Approved By:** State who approved the policy. For example: the board of directors, board sub-committee or executive management.
- **Effective Date:** The date the policy became effective.
- **Last Revision Date:** The date the policy was last revised
- **Department Responsible for Updating the Policy:** State who is responsible for reviewing and updating the policy.

Purpose

A statement of need and the goal(s) to be accomplished. It answers the question "Why has the policy has been written?" It might read: "The board of directors recognizes the need to establish a security policy in order to assure the availability, integrity and confidentiality of the information processed."

Scope

The scope defines the area covered by the policy – it details whom or what the policy applies to. For example a strong password policy might include: "The strong password policy applies to all associates that access [company name] resources."

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Body

The body is the nuts and bolts of the policy and has the following components:

- **Roles and Responsibilities**

This section addresses the responsibility of all key personnel. It should include a statement or statements that define the direction and authority for the security policy. For example an IDS Policy might include the following statement: "Logs of all security tools will be reviewed on a weekly basis by the Security Engineer." It is important to use functional titles – not names. The use of functional titles will add a sense of "timelessness" to the policy – the policy will not become obsolete because Security Engineer Jon Doe has left the organization.

- **Elements**

The elements section is where all the action takes place. This section re-states the goal of the policy and details what is needed to accomplish the goal. It does not state names of people or the technology needed to accomplish the goal. Instead, it explains in layman terms what needs to get done.

For example in an Information Classification Policy this section would define the categories of information and how each category should be handled. It might include the following statement: "Information must be classified as Confidential, For Internal Use Only or Public. Information must be clearly labeled and handled consistently from origination to destruction."

- **Risk Management**

"Risk management can be defined as identifying, assessing, and appropriately mitigating vulnerabilities and threats that can adversely impact the organization's assets. Risk is often intuitively rather than critically assessed."(NetIQ) The value of information systems and the information they contain are hard to assess. In an Information Classification policy this section would discuss the ramifications of unauthorized disclosure of an organization's information. It might include the following statement: "The unauthorized disclosure or dissemination of this information is against policy and will adversely impact the reputation and security of the organization, its employees and/or its customers."

- **Compliance**

This section addresses what is acceptable and what is not. It addresses the issue of compliance and details the ramifications for non-compliance. Also, it details the escalation process to report a policy violation. Any policy might include the following statement: "Violators of this policy will be subject to disciplinary action up to and including termination."

- **Related Documents**

The section refers to other pertinent policies and procedures.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix
The appendix might include a glossary of terms or a list of acronyms that were used within policy.

Revision History
This section details when the policy was last updated and what section or sections have been modified.

Deploying and implementing the security policy

The information security policy is finally done. It is a well-written and easy to read document meant for a broad audience - from executive management down. Executive Management!? Executive management has given the policy the support necessary for a successful implementation – right? "A sound security policy starts with the executives at the top. Without management supporting security policies, they might as well be non-existent. In most instances, management is ultimately responsible for setting the 'tone' for a sound security infrastructure."(Jarmon) Management may become real supportive real quick once security has been breached.

Security can be breached in a controlled manner like during a penetration test. Security can also be breached because some one left their laptop unattended at a client site. The laptop was still there – someone just copied the confidential client information. Without management support, it is a waste of time to implement a security policy.(Jarmon) The title section of the security template is the place to proudly display executive management's approval of the policy.

Deploying the policy is a challenge. Simply announcing that the policy is complete and distributing the policy is not enough. In a large organization tracking who has been sent the policy, who has read the policy, who has accepted the policy and performing related follow-up can be a full time job. Bindview Corporation's Policy Operations Center gives the InfoSec person the ability to automatically document who has received, read and accepted the policy. NetIQ's VigilEnt Policy Center also automates policy management by enabling you to distribute policies online.

The employees will view the security policy as a hindrance to productivity. I prefer to view the security policy as a business enabler – not a business disabler. "If you make policies too restrictive or too hard to implement and comply with, they will either be ignored (not implemented) or people will find a way to circumvent the controls in the policies."(Guel)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Monitoring compliance

Monitoring policy compliance is another challenge. There are products available that will help ease the stress of monitoring policy compliance. Bindview Corporation's bv-Control or Symantec Corporations' Symantec Enterprise Security Manager can help monitor security policy compliance by providing an automated method of assessing compliance. For example a password policy might state "passwords that are blank or are equal to the user name are not allowed." In order to monitor compliance with the password policy the InfoSec person might run an exception report titled "Users with Empty Passwords" or "Users with Password Equal User Name". Remember to report on the exception because the exception does not comply with policy. NetIQ's VigilEnt Policy Center also automates policy management by enabling the InfoSec person to automatically track and report compliance.

Who is enforcing the security policy?

"While a company's security team is ultimately responsible for generating security policies, some of the onus for enforcing them should fall on department managers."(Moore) Every department head is responsible for ensuring that his or her employees are aware of the security policy. The policy should clearly state who is responsible for enforcing it and it should list contact information.

Risk Acceptance

In rare instances, exceptions to security polices are permitted. It is necessary to document this exception by requiring the user to sign a "risk acceptance document". A member of executive management should also countersign this document so everyone understands the possible ramifications and accepts the associated risk .

Maintaining the security policy

Once a policy is created and implemented it should not be forgotten. Again, smaller, issue specific polices are easier to maintain. I feel policies need to be treated much like you treat your vehicle – policies need scheduled routine checkups and validity checks. Bindview Corporation's Operations Center also contains a policy update feature. A security policy is a living document that needs to change as the organization changes.

End User Awareness and Training

Users need to be educated. How can they be expected to follow the rules if they do not have the rulebook? Employees are familiar with physical security: video

© SANS Institute 2003, Author retains full rights.

cameras and monitors, picture id badges and limits on physical access to areas within the building (operations center, telephone room).

Employees must be aware that security policies exist and have access to them. The policy cannot be fully effective until the users fully understand and comply with the policy. "Security must be deeply embedded within the organization as a core value. A half-day awareness course or the new-hire security module simply won't cut it. All employees should feel that security is a primary responsibility."(Kirkwood) The user needs to understand that information is not "just data"; it is an asset and needs to be protected.

If the user does not fully understand the value of the information, he/she can unintentionally compromise the information. A user must understand that a strong password is the first line of defense in protecting the information and the information system. Users must manage passwords properly and be on the look out for social engineering. It might be a good idea for InfoSec to stress in the password policy that "Members of InfoSec will not ask for a user's password."

Some suggested methods for increasing employee awareness are: a banner page, a newsletter or an InfoSec page on the organization's Intranet. "Once everyone is trained, you have to have everyone sign off on [the policy] every year. Give them an updated version, educate them on what the changes are and have them sign something saying they agree to comply. Any method will work- as long as the education takes place."(Moore)

Security Procedures

"Procedures are an adjunct to policies: they are step-by-step instructions for carrying out operational tasks. A procedure will often be the instrument by which a policy is converted into action."(Robiette) Security procedures are specific operational steps that must be executed in order to achieve a certain goal. Policies define what resource is to be protected while procedures define how to protect the resource. A few security procedures that should be standard in any organization are: end user maintenance, backup and offsite storage, disaster recovery, incident response, server configuration and workstation configuration. It is important to note that not every security policy has a corresponding procedure.

Summary

When I was reading the "10 Tips for Creating a Network Security Policy", I noticed that the ten tips really brought together all of the research papers that I had read. Here a few of them: (Dulany)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Identify and locate your assets - This pertains to both information and material goods. Assess the importance and value of these assets.
- Adopt a "Need to Know" philosophy - Things like Access Control and privilege should not be a measure of rank or importance in other areas.
- Institute a standard for classifying all information - Is it confidential, private, unclassified, etc., and a means to identify which employees, or group of employees have access to this information.
- Understand that the implementation of any security policy needs regular validation – Security audits need to be performed to determine if the policy is meeting it's objectives. If it isn't, then the problems must be addressed.

A policy should outline a certain security topic, why it is important and explain what is allowed and what is not allowed. It should be general enough that changes are not required too often and it should contain general directives that are not technology dependent. By reading the policy the employee should get a clear understanding of what disciplinary measures to expect if he/she violates the policy. "The bottom line for policies is they must take into consideration the balance of protection with the level of productivity hit. You also want policies to be concise and easy to read and understand."(Guel)

"Organizations need security policies and procedures to enforce information security in a structured way"(Symantec). An effective Corporate Information Security Program is not something that can be done in a day or two. An effective program includes security policies and procedures, an end user awareness and training program and a maintenance schedule that requires the review, validating and updating of existing security policies and procedures.

"The success of the program will depend on the support of executive management and the awareness of the employees in the organization."(Singapore IT Security Techno Portal) A Corporate Information Security program is essential for securing an organization's information and information system.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

List of References
(URL access date indicates last access to check for availability)

"10 Tips for Creating a Network Security Policy." 16 October 2002. http://www.secinf.net/policy_and_standards/10_Tips_for_Creating_a_Network_Security_Policy_.html (February 2, 2003)

Berg, Al. "6 Myths About Security Policies." Information Security. October 2002 (2002): 48-56.

Bindview Corporation
www.bindview.com

Dulany, Kevin M. "Security, It's Not Just Technical." 15 January 2002. http://www.sans.org/rr/policy/tech.php (February 2, 2003)

Fraser, B. editor. "RFC2196 Site Security Handbook." September 1997. http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2196.html (February 2, 2003)

Guel, Michele D. "A Short Primer For Developing Security Policies." 2001. http://www.sans.org/resources/policies/Policy_Primer.pdf (February 2, 2003)

Jarmon, David. "A Preparation Guide to Information Security Policies." 12 March 2002.
http://www.sans.org/rr/policy/prep_guide.php (February 2, 2003)

Kauer, Harbinder. "Introduction and Education of Information Security Policies to Employees in My Organization." 23 August 2001.
http://www.sans.org/rr/aware/infosec_policies.php (February 2, 2003)

Kirkwood, John. "The Hardest Part of Security Is…" Information Security. September 2002 (2002): 30-32.

Moore, Meg Mitchell. "Pillars of Your Community." CSO. January 2003 (2003): 45-48.

NetIQ
www.netiq.com

Robiett, Alan. "Developing an Information Security Policy." 19 February 2001. http://www.jisc.ac.uk/pub01/security_policy.html (February 2, 2003)

Singapore IT Security Techno Portal. "How to Develop a Network Security Policy." 16 October 2002.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

http://www.secinf.net/info/policy/netsec1.htm (February 2, 2003)

Symantec Corporation. “Importance of Corporate Security” http://securityresponse.symantec.com/avcenter/security/content/security.articles/corp.security.policy.html

Symantec Corporation www.symantec.com

Tucker, Todd. “Security Awareness Index Report: The State of Security Awareness Among Organizations Worldwide.” 2002.

© SANS Institute 2003, Author retains full rights.

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event