Interested in learning more about security?

SANS Institute
InfoSec Reading Room

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

Security, It's Not Just Technical

The goal of this paper is to introduce the need for an adequate information security policy within your respective workplace or organization. I will also show the basic types of security policies, the basics on how to construct an information security policy and the hierarchical structure needed to implement and enforce these policies.

Copyright SANS Institute
Author Retains Full Rights

AD

Security, It's Not Just Technical

Kevin M. Dulany
GSEC Practical Assignment (v1.3)
15 January 2002

Abstract:

The goal of this paper is to introduce the need for an adequate information security policy within your respective workplace/organization. I will also show the basic types of security policies, the basics on how to construct an information security policy and the hierarchical structure needed to implement and enforce these policies.

Body:

Thousands of people transition from one job to another every day. During the check in process of the new job, they must learn the practices and procedures of their new company. One way of doing this is to review company policy. There might be a policy that states you must sign an end user agreement so you understand their internet usage, password management, and so on. The severity of each policy is inherent to the risks associated to the threats and vulnerabilities that the company has identified. There are many types of threats (natural, unintentional, intentional) and vulnerabilities (technical and administrative) and the countermeasures employed to reduce their impact. Of course, countermeasures can be technical (virus software, IDS's, etc) and/or administrative. I will to discuss an administrative countermeasure called policy.

What is a security policy? It is the set of security rules governing an Information System (IS) that provides an established level of protection. These policies must address the management, protection, and resources associated to the information and the IS. The strictness (or lack thereof) of the policies is usually established by the level of risk that the governing authority is willing to accept.

After reading SANS' "The 7 Top Management Errors that Lead to Computer Security Vulnerabilities," the first place to begin is to upgrade your security professionals within your organization. Upgrade means to hire new "trained" security professionals or "fork out" the money to train the members you currently have. Either way, this is a must and definitely the first step. So why is this first? Because you can't write a policy on security if you don't understand security!!! With this in mind, I will review the different types of security policies.

There are many types of security policies and many interpretations to those types so I will describe a few policies as defined by my references. The first set of types is depicted in "Internet Security Policy: A Technical Guide - Contents". They are 'Program Policy', 'Issue-Specific Policy' and 'System-Specific Policy'.

1. **Program Policy:** "Sets organizational strategic directions for security and assigns resources for its implementation." This is the overarching company policy that establishes your network/information security within your company. It should be very high level but detailed in the means of articulating the hierarchical structure and consequences. Program policies should be long lasting and the need for changes should be minimal over a long period of time.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

2. **Issue-Specific Policy:** "Address specific issues of concern to the organization." This is the policy that seems to be created for issues not specifically covered within the Program Policy. It could also be to address a specific issue currently exposing your company. These policies are more direct and focused. Normally, they will need to be modified depending upon the change in the threat. For example, an issue-specific policy could be for password management, contingency planning, etc.

3. **System-Specific Policy:** "Focus on decisions taken by management to protect a particular system." This is the policy that pertains to a specific system. This is the "how to" guide for a system.

The next set of policy types is from "The CISSP Prep Guide". It depicts the above in different categories and adds three elements for policy implementation.

- **Senior Management Statement of Policy –** This is the first policy that is a general, high-level statement that contains the following elements:
    - An acknowledgement of the importance of the computing resources to the business model
    - A statement of support for information security throughout the enterprise
    - A commitment to authorize and manage the definition of the lower level standards, procedures and guidelines.

The security program will fail if you do not have the senior management commitment.

- **Regulatory Policies –** These are security policies that an organization is required to implement, due to compliance, regulation, or other legal requirements. Regulatory policies commonly have two main purposes:
    - To ensure that an organization is following the standard procedures or base practices of operation in its specific industry
    - To give an organization the confidence that they are following the standard and accepted industry policy.

- **Advisory Policies –** These are security policies that are not mandated but are strongly suggested, perhaps with serious consequences defined for failure to follow them (termination, a job action warning, etc).

- **Informative Policies –** Policies that exist to inform the reader.

The Three Elements for Policy Implementation

- **Standards –** Standards specify the use of specific technologies in a uniform way. The example the book gives is the standardization of operating procedures.
- **Guidelines –** Similar to standards but are recommended actions.
- **Procedures –** These are the detailed steps that must be performed for any tasks.

You can see similarities and differences between these resources. Both have credibility and try to explain the same issues in a different manner.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The next section will try to walk you through the steps of implementing a security policy.

"Network Security Policy: Best Practices" breaks out the process of implementing a policy into 3 phases, preparation, prevention and response. Let's take a look at this.

Their preparation phase is:

- Create Usage Policy Statements

This is the establishment of the policy foundation. Start with your overarching program policy. Ensure that you identify roles and responsibilities for this program. Everyone must know who the overall authority is and any other individuals who have a designated responsibility within this program.

Remember, without senior management commitment, your policies will be useless.

- Conduct a Risk Analysis

This is the process of identifying your network's vulnerabilities, what are the current threats, and what countermeasures have you employed? Create some type of metrics that identifies the level of risk and a scale to judge it off of. This will allow for the senior management to make a logical decision on whether or not to allow the system to operate.

- Establish a Security Team Structure

This is the structure that is dedicated to the security of your company's networks. They are the policy writers and implementers. The have to work regularly with the operational departments within your company to ensure that the operational commitments and the company's commitment to security compliment each other. Many times, security is not implemented due to the cost or the possibility that the company would not be able to support their customer base. That is why security teams must work with the sections to development solutions that meet the needs of all.

Their prevention phase consists of:

- Approving Security Changes

Configuration Management is vital in the securing of an enterprise network. If you allow multiple configurations, you must ensure that your security policies cover all of these configurations. When it comes to changes, this must be a group effort and must be done in a very organized manner. Your security team must sit down and review the proposed security change. From there, they must make a recommendation on this security change to the senior management (or to the official within the company that the senior management has given the authority to make such decisions).

- Monitoring Security of your Network

The detection of change to your security posture is the key to this area. The concept here is to check the high-risk systems often (possibly hourly to daily), the medium risk systems every week, and the low risk systems monthly. Accordingly, you should have a policy in place to dictate when these checks are to be performed and by whom.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Their response phase consists of:

- Security Violations

Once you have detected a security violation, you must know how to respond it. You should create a policy that covers the reporting and handling of these violations. Your goal is to get your network back into a secure mode so act quickly. You must find out the severity of the incident and act accordingly. Make sure you document every move you make. This information can be used later to find out if your procedures are noteworthy or have room for improvement. This documentation must be accurate just in case your company has legal issues to deal with because of the incident. You should get your legal department to review your policies and information gathering techniques.

- Restoration

This is the forgotten policy topic. After a security incident happens, you want to ensure that you restore the system to a known secured state. Your procedures for backing up your servers, files, etc. must be clearly depicted in policy. Your policy should also challenge the users to keep their own backups. You should also test your backup procedures to ensure that the backups are good, that you have the resources to recreate the system from back-ups, and to ensure that they are actually being done.

- Review

Review three target areas: Policy, Posture, and Practices. You should always review your policies at the minimum, at least once a year. This will ensure that your policies are up to date and accurate. You should always be checking your security posture to ensure that the defense in depth methodology you have employed is secured. The practices one is about keeping your users aware of the policies and best security practices that they can do so they can do their part in security. The users have been know to be a major threat to your networks and the more you can train them on these practices, the better chance you have of reducing the severity of the threat.

From the references noted and others not listed, I have noticed numerous similarities to the content of a security policy. I will show you my "basic security template" and explain each section.

TITLE:
The title of the policy should be "straight, direct, and to the point".
Example titles could be:
"[Company Name] INFORMATION ASSURANCE PROGRAM"
"[Company Name] PASSWORD MANAGEMENT POLICY"

PURPOSE:
The purpose section must tell the target audience why this policy is being written. It must depict the security objectives you are trying to meet.
Example purpose statement for implementing a password policy:
"The purpose of this policy is to set the minimum standard for authenticating to all applications and networks owned and operated by [Company Name]."

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

BACKGROUND:
This background section is usually lengthy but needed. It supports the purpose section. It should articulate the problem from inception up to the current state and identify the threat or vulnerability that this policy is addressing.

REFERENCES:
This section is crucial. You should always identify higher-level company policy that this policy supports. If possible, you should also identify any public laws that this policy addresses also.
Examples:

- Computer Security Act
- Electronic Communications Privacy Act
- Freedom of Information Act
- [Company Name] Internet Usage Policy

CANCELLATIONS:
This section needs to be there if the new policy cancels another policy. Dependant upon the distribution of information within your organization, there are times when new policy doesn't filter down to all of the sections within your organization. For example, you create a new policy addressing password management. Your old policy stated, "All passwords will be at least 6 characters in length." Your new policy was written due to address the threat of the new password cracking software availability and you want to strengthen all passwords to 8 characters utilizing multiple character sets (upper case, lower case, numeric, special characters, etc). If one section still thinks that the old policy is still in effect, your company is still vulnerable. My point is to ensure that the distribution of the policy is accurate and timely to ensure that everyone is using up to date references.

ROLES AND RESPONSIBILITIES:
This section must identify who is responsible for the security of the system and who within your organization is affected by this policy.
An example is could be like this:
CIO Section - "You are responsible for the implementation of this policy"
Head, Training Section – "Ensure the appropriate training is available for all employees on this policy"
All Employees – "All employees are responsible for following this policy"
Note: When identifying the roles and responsibilities, always ensure that you identify billets vice individual names. This will ensure that you will not have to re-write the policy every time someone gets promoted or leaves the company. If the need exists to identify individual names, ensure that you address this in an enclosure or appendix vice the actual policy.

EFFECTIVE DATE:
Ensure that you clearly identify when this policy takes effect. The norm is to state that this policy is in effect upon signature.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

EXPIRATION DATE:
You should always put an expiration date on a policy even if no logical date exists.

POLICY/EXECUTION:
This is the meat and potatoes of any policy….the actual verbiage depicting what can or cannot be done and must address the consequences for not complying. This must be detailed to the intent of the policy.
For example, if we go back to our password management policy that we talked about earlier, this section might say:

- The minimum length of all passwords for the <system name> will be 8 characters.
- This password must contain at least one upper case character, one lower case character, one numeric character and one special character.
- All passwords will be changed every 90 days.

ENCLOSURES/APPENDIXES:
Enclosures and appendixes are used to support the overall document. If your policy uses a numerous amount of acronyms, you could supply a listing and make it Appendix A. This is also useful for definitions and maps.

We touched on the many types of policies and a process to walk you through the implementation of security policies. Let's look at some "tips" for creating a security policy.

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 are a few of them:

1. **Identify and locate your assets.** – You must know what you have and where you have it. Security professionals are always reviewing information of published vulnerabilities and threats. If your Company uses multiple operating systems, you must ensure that your research is all-inclusive.
2. **Adopt a "Need to Know" philosophy.** – Great concept. Ensure that you have a process for giving users access to specific information and location. This also referred to as the principle of least privilege.
3. **Institute a standard for classifying all information** - Create the classification levels for your company's information with proper handling procedures. Then, make sure that all of your company's information is labeled and protected within the classification levels you created. A basic set of classifications would be Public, Private, and Confidential. Each would have specific handling procedures (i.e. No Confidential information will be sent out to .com email addresses, etc.)
4. **Review the impact of any intended procedural changes on your employees.** Prior to implementing a security policy, you must find out what the impact will be on your employees. You must always educate your target audience on new policies and procedures. This can be done by either creating a handout for the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

users to read, or create a training package for them to sit through. This is crucial when you invoke new procedures.

5. **Understand that the implementation of any security policy needs regular validation.** This is a must!!! You must regularly monitor your policy for compliance and accuracy.

Pertaining to security, the following some of the areas where policy must be created for:

- The establishment of the hierarchical structure for you organization.
- Physical Security
- Personnel Security
- Configuration Management
- Classification and Handling of Company Information – Your organization must identify the sensitivity of their internal information and the handling procedures for each level of sensitivity.
- Identification and Authentication
- Remote Access
- Contingency Planning
- Virus Protection
- Encryption
- Backup/Recovery Operations
- Incident Response
- Wireless/PEDS

The final portion pertaining to security policies is the security hierarchical structure needed. Within my organization, the president of the company appointed a Chief Information Officer (CIO). My CIO is responsible for aspects of communications and computers throughout our organization. Here is a brief depiction of how we are broken down (with security in mind):

CIO – The governing authority for all aspects of communications and computers. He has the final say of everything. His staff is broke down into divisions: Network Plans and Policy, Network Operations and branch managers

Network Plans and Policy – This is where all of the company-wide policy is written and distributed from. It contains a Network Infrastructure Section (NIS) and an Information Assurance Section (IAS). The NIS handles all aspects of the infrastructure and the IAS handles the security. We are collocated and converse on all issues regularly. The policy that comes out of here is normally high-level that normally will tell the "What we want done". Normally, the high-level policy will tell how when applicable. Otherwise, this policy will tell the local branch managers what we want done and they implement as they see fit.

Network Operations – These are the technical implementers for the company. They enforce and implement the company-wide policy. They provide the technical guidance

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

and best practices to the branch managers. They control the overall physical management of the company's enterprise network. They have internal sections for Intrusion Detection, VPN support, Certification and Accreditation, and Operations just to name a few.

Local Branch Managers – Since our company is not physically located in one building, we needed to have a local authority at every location. This manager is responsible for the day-to-day operations at his location. He must ensure that his location is in compliance with all higher-level policy. He has the authority to add additional security measures to his location dependent upon the local threat. Each local branch has security professionals on staff.

SUMMARY: I have tried to assist you in the development and implementation of security policies. If you transition from company to company, you will probably see many similarities and differences in policies, procedures, and best security practices. There is no 100% solution to security!!! If you develop you security program utilizing a defense in depth model, your overall security posture will be enhanced. Defense in depth is the concept of using a layered approach to security. Starting from your outer boundary to the end user and every aspect in between. It is much like the concept of a defense in football. Each layer has individual responsibilities and together with the other layers, provides the necessary security needed stop the opposing attack. The ultimate decision-makers of the world are starting to put more emphasis on security due to recent events but usually, do not initiate security until they need to (i.e. virus software). We as security professionals must take a more proactive approach to ensure the confidentiality, integrity, and availability of our information and information systems.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References:

1. "How to Develop a Network Security Policy" http://www.sun.com/software/white-papers/wp-security-devsecpolicy/
2. "The 7 Top Management Errors that Lead to Computer Security Vulnerabilities" http://www.sans.org/newlook/resources/errors.htm
3. "10 Tips for Creating a Network Security Policy" http://secinf.net/info/policy/10tips.htm
4. "Internet Security Policy: A Technical Guide - Contents" http://secinf.net/info/policy/isptg.en/ISPTG-Contents.html
5. "Network Security Policy: Best Practices" http://www.cisco.com/warp/public/126/secpol.html
6. "Network Security Tutorial - Part IV" http://netsecurity.about.com/library/weekly/aa080299.htm?once=true&iam=mt
7. "Hackers Beware", Eric Cole
8. "The CISSP Prep Guide", Ronald L. Krutz

© SANS Institute 2002, Author retains full rights

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**