Global Information Assurance Certification Paper

Security Policies –
A Management Perceptive

GIAC Security Leadership Certificate

GSLC Assignment 1.0
(April 8, 2002)

Author: John Franco
Date: 09/09/2003

Security Policies – A Management Perceptive

Abstract:

Security policies may not be the beginning and end-all of a good security, however they are what management can use to ensure that the people, systems, and the information that they store are protected. While it is said that security is the responsibility of every employee, if security is going to be effective, it must flow from the top down. As stated in the All-In-One CISSP Certification Exam Guide, pg 59 "In the world of security management's functions involves determining objectives, scope, policies, priorities, standards, and strategies.", this paper is to present the development of a security policy.

It is important to understand that good policy makes for good security, knowing this will go a long way in keeping your data secure. Additionally, it is important that we don't get discourage and not follow though with the development of a security policy, many policies are started but never followed through or ever get published or signed by senior management. Remember, without a security policy, you will not be able to enforce good security.

Introduction:

Now that I have your attention, let me explain what a security policy is and what it is not. A security policy is a plan, a road map of what the organization considers good security and what measures are needed to protect the confidentiality, integrity, and availability of the data and the systems that the organization are responsible for. A security policy should be set up so that it first protects people and information. As stated in one of the SANS training manuals. "A well written policy contains a sufficient definition of "What" to do so that the "How" can be identified and measured or evaluated"

What a policy is not – it is not a set of procedures or methods on how something will be done. A policy is not the standards by which things are to be done, or are they the guidelines in which things are to be done. Security policy generally states what needs to be done and why it needs to be done, a separate document will explain the how.

You can say that a security policy is the who, what, and why, of security, but the when, where and how are left to the standards, procedures, baselines, and guidelines that will be referenced in the security policy.

A good security policy must address the issue of enforcement, what needs to be done, what reference materials are to be used, who will be responsible to see that it is done, and what are the penalties for violation of the policy.

As you can see, without a security policy – your staff will be setting security up the way that they think it should be done. If your staff is highly security minded this may not pose a problem, however, if your staff is under the gun to get things going, security is most likely the first area that will be overlooked or dropped. In addition to this, there are regulations for certain industries that will require that you have security policies.

Types of Security Policies

Security policies generally fall into three areas, they are:

Organizational or Program Specific – these are the policies that deal directly with the organization or program as a whole. They define the over-all affect that security will have throughout the entire organization or program, whether the security will be tight and enforceable. These policies state the laws and regulations that pertain to the organization or program. These are the highest level security policies; they define the overall goals and enforcement of security.

Issue Specific – These are the nuts and bolts of security policy. These are the polices that deal with everything from how you will deal with email, system passwords, to system backup and recover and data retention.

System Specific – This type of policy will refer to a specific system. This being how certain operating systems will be hardened, or protected. How certain types of databases will be secured. Policy define a set of approved software that would be allowed on a system would be an example of a system specific policy.

What Makes a Good Policy?:

While there may be many ways to develop a good policy there are some key areas that are universally agreed upon that make a policy good. These are a compilation from many authors and security how to book, several which are in the reference section. They are:

a- **Clearly written** – a policy that is clearly written will be one that the average employee will understand. What use is a policy that is written in legalese or computerese while most of the organization has no idea what the policy is for.

b- **Enforceable** – in order for a policy to be effective and good, it must be enforceable. Defining in the policy how it will be enforced, who will be responsible for ensuring that the policy is followed will go a long way in letting the employee know what the consequences are for voliation od said policy. Please note that it is very important that you run this by your Human Resource and Legal department before issuing the policy.

c- **Easy to comply with –** if a policy is easy to comply with, you will have greater buy-in and compliance with the employees. If you put too many rules and make it difficult for people to do their jobs, they will find ways to circumvent the policy so that they can do the work that they have been paid to do. A good security policy should not be one that prevents someone from doing their job, but allows them to do their job while protecting the assets of the organization.

d- **Not objectionable to most people –** the policy that you write should be one that most people in the organization can agree with. There is no use putting a lot of effort into a policy that most of your employee will not follow. Once again, if a policy is stupid and places undue burden on your employees, they will find a way to get around it. When writing the policy, you can clearly make a defense for it by spelling out the reason for the policy and the legal requirements of the policy. If you can do a good job at that, most people will not object and you will have buy-in.

e- **Easily accessible by all –** what good is a policy if most of your employees don't know about it, or don't have access to it? You can't expect to enforce a policy that no one knows about. You can ensure that all employees know about them and where to find the policies by having all employees attend or complete Computer Security Awareness training. Doing something like this once a year can help ensure that all employees have the opportunity to find out about the policies. Work with your Hunan resource department to ensure that access to the computer security policies are part of the employee handbook.

f- **Up-to-Date –** once a policy is written and all your employees know about it, the policy needs to be kept up-to-date. A good practice is to put a self expiring date on the policy. Another good practice would be to have an annual review of polices to see if they still pertain and are relevant to the organization. Having an outdated policy, or several policies on the same topic can cause confusion to the employees and prevent they from following the correct policy.

g- **Consequences -** finally, to have a good policy we have already stated that it should be enforceable, however the policy should clearly state the consequences for violation of the policy. Be sure that you run this by both your Human Resource department and your legal department.

Policy Development:

Before putting pen to paper the first thing you must do in policy development is to determine what you are trying to protect and then determine whether or not there are existing policies that cover what you would like to accomplish. If there are policies already, do they address all the issue? Have they been reviewed and signed by management? Are they enforceable? Are the policies known by the

staff and do they understand the intent of the policy. It would be very difficult if your organization had a policy on personal use of company computers if none of the employees knew about the policy?

If there are no policies in your organization, then the very first policy would be an Organizational or Program type policy. Here you would define the overall scope of what security means to your organization, management's role and commitment to security, along with who is responsible for security, and what the legal requirements are, such as the federal regulations that pertain to your industry.

After you have the organization security plan, you will need to discover what the "family jewels" are? Family jewels are those systems and data that are core to your survival as a company, would cause embarrassment if leaked, or data that you are legally responsible to protect. For Coke-a-Cola it would be the secret formula for their syrup, they sure wouldn't want Pepsi to get hold of it. In a hospital or bank – access to either the patient or account holder's data would be considered the family jewels.

Once you have identified the family jewels, you will have a better idea of what you need to protect and how you can protect it. The best way to determine what needs to be protected is to do a risk assessment. The risk assessment will allow you to see what the systems are within your organization and what the vulnerabilities are to those systems. This will also allow management to see which issue specific and system specific policy needs to be written or needs to be updated. So it is very important that senior management be updated with the results of a risk assessment, remember, security is a management responsibility.

Assuming that your organization is a hospital some of the items that you would need to protect would be the patient's medical and financial records. You know that the data resides on systems within your IT department. You would need to look at the federal regulations covering hospitals and patient information. Here you would discover that Health Insurance Portability and Accounting Act, or better known as HIPAA tells you what you what you need to protect and it will also define some standards that you will need to meet the regulation.

When developing a policy, they should be based upon protecting the data in the following ways:

- **Confidentiality** – here you need to insure that access to the data is seen or used only by those that are authorized to see the data. Authorization is normally done by the owner of the data, they will define which people and/or systems can have access to the data and to what extent they can have access.
- **Integrity-** here you must insure that the data is the same throughout the life of the data, that the only changes, modifications, or deletions to the

data have been authorized. You must insure that the data can only be changed, modified, or deleted within the scope of what the data owner has authorized

- **Availability**- insuring that the data is available to those that have been authorized to see the data and that it is not available to those that have not been authorized.

All security policies should be based upon those three items

Management and the owners of the systems will need to develop methods to verify that compliance with the policies has been achieved.

Remember that a security policy is defining what needs to be protected and why it needs to be protected. Some documents that are referenced by a security policy that will help in ensuring that compliance has been met are:

1- **Standards –** define what will be the hardware and or software to be used – this could be that all back-up will use a specific software package, or that all firewalls will conform to a certain standard.
2- **Procedures –** these are the step by step method that will be used, how things will be done, how backups are to be done, when they will be done, etc.
3- **Baselines –** these are the minimum configurations or steps that must be followed. This could be that all machines would be at a certain OS level or that all passwords will a certain length.
4- **Guideline –** these are recommendations or 'Best Practices".

Conclusion:

In conclusion, it is management responsibility to set the overall tone for security. Management has the obligation to protect the people and information that has been entrusted to them. There are federal regulations that cover many industries, such as Healthcare and Banking that management has a responsibility to ensure that they are compliant with. Management can ensure that they are on the road to compliance if they have a good security policy.

The first and foremost policy should be the Program or Organization specific policy, followed by Issue and System specific policies.

Policies define the who, what, and why. The when, where and how are defined in the standards, guidelines, and procedures that will be referenced from the policy.

A good policy will be one that is clearly written, enforceable, easily accessible to the users, has buy in from your users, is up-to-date, and has clearly spelled out consequences.

Last but not least - Security Policies assist you in protecting the Confidentiality, Integrity, and Availability of the data that make up the family jewels of your organization.

References:

Importance of Corporate Security Policy - Symantec
http://securityresponse.symantec.com/avcenter/security/Content/security.articles/corp.security.policy.html

Enforcing a corporate security policy – Network Magazine
http://www.networkmagazineindia.com/200111/focus4.htm

Tipton, Harold F., Krause, Micki. Information Security Management Handbook – 4th Edition, Auerbach, 2000,

Hutt, Arthur E. Bosworth, Seymour, Hoyt, Douglas B., Computer Security Handbook, 3rd Edition, John Wiley & Sons, Inc, 1995, 2.2

Jenkins, George, Wallace, Michael. IT Policies & Procedures, Tools & Techniques That Work. Prentice Hall, Paramus, NJ 070652, 2002, 3-5

Harris, Shorn. All-in-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Berkley, California, 2002.

SANS Institute – Track 9 – Information Security Officer Training 9.4 Information Security Policy: A Roadmap for Security Officers, 2002

Last Updated: May 28th, 2017

Upcoming Training

SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
Community SANS Seattle MGT512	Seattle, WA	Aug 14, 2017 - Aug 18, 2017	Community SANS
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS New Orleans MGT512	New Orleans, LA	Aug 21, 2017 - Aug 25, 2017	Community SANS
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS New York MGT512	New York, NY	Aug 28, 2017 - Sep 01, 2017	Community SANS
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Toronto MGT512	Toronto, ON	Sep 18, 2017 - Sep 22, 2017	Community SANS
Community SANS Columbus MGT512	Columbus, OH	Sep 25, 2017 - Sep 29, 2017	Community SANS
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced