Global Information Assurance Certification Paper

Network Security Policy – A Manager's Perspective
Ernest D. Hernandez
November 22, 2000

As all GOOD and COMPETENT managers of people know, it is the people who work for you that determine the success of whatever endeavor you are undertaking. In the field of Network Security it is no different. It will be your network people and users that will either help keep your network secure, or cause problems that could lead to serious information compromise, or financial loss. The tool that a Network Manager has to facilitate and manage good Network Security is policy.

Putting an effective, credible and adapting Network Security Policy to paper can be a very challenging endeavor. Depending on the size of your network, it may be just you, you and a select committee of key people, or for very large organizations, an internal security department. Regardless of whoever is in charge, a "Security Committee" should be formed for the expressed purpose of developing, and just as important, continuously evaluating the Network Security Policy. The following list is provided as a general guideline and is dependent on the size of your organization:

- Network Administrator
- Security Administrator
- IT staff (technicians, analysts, programmers, etc.)
- Department Heads and Managers
- Human Resources
- Legal Staff

Note that not everyone need be computer literate. While it would certainly help to have everyone understand what is and is not possible through the hardware and software on your network, it will immensely improve the credibility of your policy if you include folks who may not completely understand computers, but have a stake in how the policy is determined.

To expand a bit on the above, all GOOD and COMPETENT managers of people also know that if you are to positively affect the behavior of people through policy, you must get the key stakeholders of your organization to buy into the policy you are developing. Whether these are upper level managers, company department heads, clients, or end users, their interest should be represented when forming policy. In this way less resistance will be encountered when implementing the policy, and just as important, you will be able to get feedback on how effective the policy is. It is important to stress that upper management buy-in is key here and this is where it needs to happen. Without upper-level management approval, the Network Security Policy cannot be implemented or enforced.

Writing the actual document requires a good deal of research and gathering of information. A comprehensive guide to writing a Network Security Policy can be found in RFC 2196 at http://info.internet.isi.edu/in-notes/rfc/files/rfc2196.txt. As a minimum, the following steps should be taken before beginning writing the policy:

- Identify the risks that threaten your company's network.
- Find out what managers and other employees expect from the company's network resources and from each other.
- Read network security policies from other companies – preferably from companies similar to your own.

The first step is to conduct a *risk assessment*, which is an evaluation of your network to determine which assets are worth protecting and the extent to which these assets should be protected. A list of tangible and intangible assets needs to be made. The list needs to include all your network hardware as well as the software, data and information stored on your network. The latter is the intangible part of your assets. To more effectively inventory your intangibles, produce a printout of each server's directory structure and identify those directories that hold confidential and mission-critical data.

After completing the inventory, determine how much your organization would have to spend in terms of time and money to replace each asset. As an example, information on a break-through technology that can produce millions for you, or a competitor, should be valued appropriately. Rank these assets by their relative values in terms of time and money it would take to replace them. This prioritized list will help focus the writing of security measures that best protect your most valuable assets without getting bogged down on assets of lesser value.

With list in hand, evaluate *each security threat*, determining the likelihood of the threat occurring to each of your assets. This is where a thorough knowledge of the threats to your assets is needed. If you're concerned about Internet threats, you need an expert in that field. If you're concerned about natural disasters (earthquakes, flooding, fire) you need expert information in that area on protecting your assets. A thorough risk assessment, with the requisite expert information included, will be the most valuable tool in shaping the Network Security Policy.

Your second step is to survey your organization's users to find out what level of network security they expect and what assets they feel should be protected. Though your security committee includes representatives throughout the organization, a survey of this kind could very well reveal issues that were overlooked. An anonymous survey could further reveal issues that committee members are unwilling to express in public.

A survey that includes all users (managers included!) will help determine which assets are used frequently and by whom. The results can

help in prioritizing the protection of assets. Those used more get more protection and those used less get less (depending on the value of data on them of course).

This survey can also resolve a contentious issue occurring in many organizations, the proper use of company assets by employees. The survey can go a long way in adding credibility to your policy. Employees can be surveyed on what assets they would like to use and why they would need to use them. Additionally, managers can be surveyed on how they feel about employees using company assets. Again, this will facilitate user buy in and significantly increase policy acceptance.

The third step is to review the network security policies of other organizations, especially those that share similar characteristics to your own. Depending on how successful or unsuccessful those other companies are in securing their network, an analysis of how these other organizations dealt with issues included in their policy could help in formulating your own policy. You can pick and choose among other organization's policies those aspects that would suit your organization (i.e., physical security, disaster recovery, incident handling, etc.). You can find several network security policies in the Computer Operations, Audit and Security technology (COAST) archive at http://www.cs.purdue.edu/coast.

Once a Network Security Policy is written, the job of managing and implementing security is not over. The security committee used to formulate the policy is the mechanism by which the policy is evaluated and modified if need be. A month or two after the initial introduction of the policy, the security committee can discuss which parts of the policy are effective and which parts need to be revised. They can also address any grievances brought forward as a result of implementing the policy. Additionally, as new equipment, technology, threats and situations arise, the security committee can convene to address those concerns.

Finally, to ensure the success and effectiveness of a Network Security Policy, the following three elements need to be included and emphasized:

- Management Support
- User Training
- Cost-effective Security Measures

As alluded to earlier, the most important element in a successful security policy is management support. When upper management buys into and makes a firm statement that network security is important, users throughout the organization will take the security policy seriously. If managers support the security policy, they will also support penalizing users who violate this policy and include adhering to security policy as part of annual performance reviews.

To further facilitate buy-in among users and increase the credibility of the security policy, users need to be trained on all aspects of the policy. Training should focus on how the security policy protects the assets of your organization and what happens if the policy is not followed (both as a consequence to company assets and employees viability within the company). Managers should do what ever it takes (within reason and fiscal constraints) to encourage users to follow the organization's network security policy.

Cost-effective security measures mean that you should never spend more money to protect an asset than the asset is worth. A review of the risk assessment done before the security policy was written will indicate an asset's worth. Periodically compare the measures taken to protect that asset and ensure the measures do not cost more than the asset. This way upper management will see that the security policy is truly cost effective.

With a well written, thought out Network Security Policy, you can automatically set into motion the actions needed to secure your assets from disaster, intruders (both within or outside the organization), and to routine tasks. While a very basic outline of a security policy was given here, a good security policy outlines the appropriate responses to all aspects of the organization's network. The policy also permits your network people to do their jobs more effectively and without fear of jeopardizing your organization's most valuable assets, or their careers.

Sources

Fraser, B. "Site Security Handbook." Request for Comments: 2196. September 1997. URL: http://info.internet.isi.edu/in-notes/rfc/files/rfc2196.txt (20 November 2000).

Jeffress, Terry L. "Getting It on Paper." Network Security Policy. January 1997. URL: http://www.nwconnection.com/jan.97/secpol17/index.html (20 November 2000).

Jeffress, Terry L. "Three Key Elements of a Successful Security Program." Network Security Policy. January 1997. URL:http://www.nwconnection.com/jan.97/secpol17/3keyel17.html (20 November 2000).

Williams, Jim. "Network Security Tutorial – Part I." Internet/Network Security. 7 June 1999. URL: http://netsecurity.about.com/computenetsecurity/library/weekly/aa060799.htm. (20 November 2000).

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event