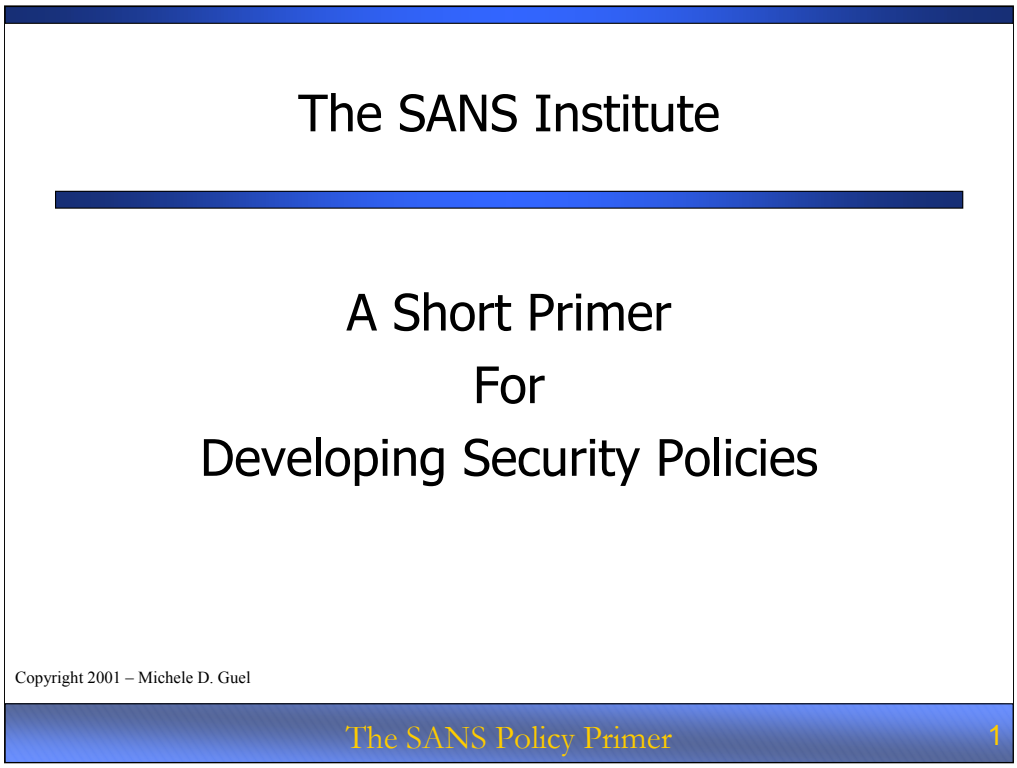

This short primer of developing security policies is taken from Michele D. Guel's full day tutorial title "Proven Practices for Managing the Security Function."

A Security Policy Framework

- Policies define appropriate behavior.
- Policies set the stage in terms of what tools and procedures are needed.
- Policies communicate a consensus.
- Policies provide a foundation for HR action in response to inappropriate behavior.
- Policies may help prosecute cases.

Security policies are an absolute must for any organization. They provide the virtual glue to hold it all together. Imagine a small city that did not have any rules? What would life be like? The same applies to your organization – policies lay the ground-work. Later this afternoon in Section 7 we will take a detailed look into the security policy framework.

Who and What to Trust

- Trust is a major principle underlying the development of security policies.
- Initial step is to determine who gets access.
- Deciding on level of trust is a delicate balancing act.
  - too much trust may lead to eventual security problems
  - too little trust may make it difficult to find and keep employees
- How much should you trust resources or people?

Before we begin our discussion about policies, lets talk a little about trust. Trust is a central theme in many policies. Some policies may not be written because there is trust that people will do the right thing. Then on the other hand, some policies are needed because we know people don't always do the right thing.

Ideally you want to trust all resources, but that is unrealistic. Buggy hardware and software are commonplace. Try to implement controls and procedures to minimize the impact when a failure does occur.

Trust of employees and users develops over time. Different categories of employees should be trusted at different levels. Ensure level of access is commensurate with level of trust.

Possible Trust Models

- Trust everyone all of the time:
  - easiest to enforce, but impractical
  - one bad apple can ruin the whole barrel
- Trust no one at no time:
  - most restrictive, but also impractical
  - difficult to staff positions
- Trust some people some of the time:
  - exercise caution in amount of trust given
  - access is given out as needed
  - technical controls are needed to ensure trust is not violated

When looking at trust, you have three basic models – those listed above. It is not very common to find organizations that follow the model of trusting everyone all of the time. In today's world it is just not possible. On the same token the model of trusting no one at no time is also not that common. This model is mostly found in high level security government organizations. The most common model is to trust some of the people some of the time and to build trust over time. Also keep in mind that it may be appropriate to apply different trust models to different parts of the organization.

Why the Political Turmoil?

- People view policies as:
  - an impediment to productivity
  - measures to control behavior
- People have different views about the need for security controls.
- People fear policies will be difficult to follow and implement.
- Policies affect everyone within the organization.

My experience in the field has consistently shown that security policies tend to elevate the level of tension in any given situation. It basically boils down to the fact that people don't like rules and don't like to be restricted in their activities. One reason for the tension level is that everyone tends to view security needs differently:

•Users are concerned about being able to get their work done without a lot of controls.

•System support personnel are concerned about the ease of managing systems under tight control.

•Management is concerned about costs versus protection.

Getting all sides to agree about the elements of a policy is nearly impossible. It is always best to try to reach a "win-win" compromise.

Who Should Be Concerned?

- Users - policies will affect them the most.
- System support personnel - they will be required to implement, comply with and support the policies.
- Managers - they are concerned about protection of data and the associated cost of the policy.
- Company lawyers and auditors - they are concerned about company reputation, responsibility to clients/customers.

Basically, everyone should be concerned security policies because everyone is affected by them to some extent. The system users are typically affected the most as they see the policies as a set of rules to regulate their behavior and make it more difficult for them to accomplish their job. The people who have to support the infrastructure are concerned since they are the ones who have to implement and comply by many of the policies. For example, a policy that requires all Solaris hosts to be installed according to a baseline security standard would require more work on the part of the system administrators. Not only for the initial install, but also for the upkeep of the system.

The Policy Design Process

- Choose the policy development team.
- Designate a person or "body" to serve as the official policy interpreter.
- Decide on the scope and goals of the policy.
  - Scope should be a statement about who is covered by the policy.
- Decide on how specific to make the policy.
  - not meant to be a detailed implementation plan
  - don't include facts which change frequently

Ideally, you should have a formal policy design process that is consistently followed for all security policies. The process would specify who develops the initial draft of the policy, which groups are required to review each policy, the required approval process and finally the implementation process.

The SAGE booklet "A Guide to Developing Computing Policy Documents", recommends:

a senior level administrator

a member of management who can enforce the policy

a member of the legal staff

a representative from the user community

someone with good writing skills

The size of the policy design group will depend on the size and scope of the policy. Small scale policies may only require one or two people while large scale policies may require a team of 5-10.

The Policy Design Process

- A sample of people affected by the policy should be provided an opportunity to review and comment.
- A sampling of the support staff effected by policy should have an opportunity to review it.
- Incorporate policy awareness as a part of employee orientation.
- Provide a refresher overview course on policies once or twice a year.

If at all possible, notify people in advance that a new policy is being developed and explain why the policy is needed.

Prior to deploying a new policy, allow people one-two weeks to review and comment.

People given responsibility in a policy should also have the authority to carry out their responsibilities.

Basic Policy Requirements

- Policies must:
  - be implementable and enforceable
  - be concise and easy to understand
  - balance protection with productivity
- Policies should:
  - state reasons why policy is needed
  - describe what is covered by the policies
  - define contacts and responsibilities
  - discuss how violations will be handled

This page discusses some basic rules for policies. While many of these may seem obvious, it is necessary to point them out. When planning policies, some organizations will go overboard with policies and come up with something that will be impossible to implement and comply with. 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. Our goal at Cisco is to keep policies to 2 pages or less, if at all possible. We do have a few policies which are 4 or 5 pages. One thing to keep in mind when developing a policy is how it will effect legacy systems and other infrastructure that is already in place. Once the policies are fully approved, they should be made available to all users who are affected. Finally, all policies should be updated annually to reflect changes in organization or culture.

Level of Control

- Security needs and culture play major role.
- Security policies MUST balance level of control with level of productivity.
- If policies are too restrictive, people will find ways to circumvent controls.
- Technical controls are not always possible.
- You must have management commitment on the level of control.

One of the major goal of a policy is to implement control. Deciding on the level of control for a specific policy is not always clear-cut. The security needs and the culture of the organization will play a major role when deciding what level of control is appropriate. 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.

Policy Structure

- Dependent on company size and goals.
- One large document or several small ones?
  - smaller documents are easier to maintain/update
- Some policies appropriate for every site, others are specific to certain environments.
- Some key policies:
  - acceptable use
  - remote access
  - information protection
  - perimeter security
  - baseline host/device security

There are potentially dozens of policy topics that may be appropriate for most mid to large size organizations.

Some of Cisco's major policies:

Acceptable Encryption
Application Service Providers
Acceptable User
Acquisition Assessment
Audit
Risk Assessment
Information Sensitivity
Password
Laptop Security
DMZ Equipment
Extranet
Host Security
Lab Security
Anti-Virus
Router/Switch
Wireless Communications
Remote Access
VPN

The Acceptable Use Policy

- Discusses and defines the appropriate use of the computing resources.
- Users should be required to read and sign AU policy as part of the account request process.
- A key policy that all sites should have.

Example policies and procedures can be found on the SANS web site at:

http://www.sans.org/newlook/resources/policies/policies.htm

The Acceptable Use policy is probably one of the most important policies a site can have. For educational and government organizations, it is basically a "must have." Without such a written policy, management and support staff have nothing they can reference when attempting to punish an employee/guest who has violated the acceptable, safe computing practices.

Some Elements

- Should state responsibility of users in terms of protecting information stored on their accounts.
- Should state if users can read and copy files that are not their own, but are accessible to them.
- Should state level of acceptable usage for electronic mail, internet news and web access.
- Should discuss acceptable non-business uses of the resources.

Some example text from a AU policy might read:

"Users are responsible for protecting any information used and/or stored on/in their accounts at <company name>. Consult the user guide for guidelines on protecting your account and information using the standard system protection methods or by use of encryption software such as PGP. Company or third party confidential information should not be be stored or transmitted to non<company name> hosts."

"Users shall not attempt to access any data or programs contained on <company name> hosts for which they do not have authorization or explicit consent from the owner of the data/information, or from an appropriate level of management."

Remote Access Policy

- Outlines and defines acceptable methods of remotely connecting to the internal network.
- Essential in large organization where networks are geographically dispersed and even extend into the homes.
- Should cover all available methods to remotely access internal resources:
  - dial-in (SLIP, PPP)
  - isdn/frame relay
  - telnet/ssh access from internet
  - cable modem/vpn/DSL

Example Text:

1. It is the responsibility of <Company Name> employees, contractors, vendors and agents with remote access privileges to <Company Name>'s corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to <Company Name>.

2. General access to the Internet for recreational use by immediate household members through the <Company Name> Network on personal computers is permitted for employees that have flat-rate services. The <Company Name> employee is responsible to ensure the family member does not violate any <Company Name> policies, does not perform illegal activities, and does not use the access for outside business interests. The <Company Name> employee bears responsibility for the consequences should the access be misused.

3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of <Company Name>'s network:

a. Acceptable Encryption Policy

b. Virtual Private Network (VPN) Policy

c. Wireless Communications Policy

d. Acceptable Use Policy

4. For additional information regarding <Company Name>'s remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

Some Elements

- Should define who can have remote access.
- Should define what methods are allowed for remote access.
- Should discuss who is allowed to have high-speed remote access such as ISDN, frame relay or cable modem.
  - extra requirements
  - appropriate use
- Should discuss any restrictions on data that can be accessed remotely.

More Example Text:

Requirements

Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.

2. At no time should any <Company Name> employee provide their login or email password to anyone, not even family members.

3. <Company Name> employees and contractors with remote access privileges must ensure that their <Company Name>-owned or personal computer or workstation, which is remotely connected to <Company Name>'s corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

4. <Company Name> employees and contractors with remote access privileges to <Company Name>'s corporate network must not use non-<Company Name> email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct <Company Name> business, thereby ensuring that official business is never confused with personal business.

5. Routers for dedicated ISDN lines configured for access to the <Company Name> network must meet minimum authentication requirements of CHAP.

Information Protection Policy

- Provides guidelines to users on the processing, storage and transmission of sensitive information.
- Main goal is to ensure information is appropriately protected from modification or disclosure.
- May be appropriate to have new employees sign policy as part of their initial orientation.
- Should define sensitivity levels of information.

Even though it may seem like common sense to protect company private information, many employees don't take the time to consider the sensitivity level of much of the information they see. If possible, attach a level rating to information sent out via email and interoffice mail.

Employees who work exclusively on a laptop need to be more cautious of protecting information stored on that system. Especially when traveling, where the likelihood that strangers will gain access to the laptop or steel the laptop is dramatically higher.

Some Elements

- Should define who can have access to sensitive information.
  - "need-to-know"
  - special circumstances
  - non-disclosure agreements
- Should define how sensitive information is to be stored and transmitted (encrypted, archive files, uuencoded, etc).
- Should define on which systems sensitive information can be stored.

Example Text:

All <Company Name> information is categorized into two main classifications:

- <Company Name> Public
- <Company Name> Confidential

<Company Name> Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to <Company Name> Systems, Inc.

<Company Name> Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in <Company Name> Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

Some Elements

- Should discuss what levels of sensitive information can be printed on physically insecure printers.
- Should define how sensitive information is removed from systems and storage devices:
  - degaussing of storage media
  - scrubbing of hard drives
  - shredding of hardcopy output
- Should discuss any default file and directory permissions defined in system-wide configuration files.

More Example Text:

A subset of <Company Name> Confidential information is "<Company Name> Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to <Company Name> by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into <Company Name>'s network to support our operations.

<Company Name> personnel are encouraged to use common sense judgment in securing <Company Name> Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

The Perimeter Security Policy

- Describes, in general, how perimeter security is maintained.
- Describes who is responsible for maintaining it.
- Describes how hardware and software changes to perimeter security devices are managed and how changes are requested and approved.

This page left intentionally blank.

Some Elements

- Should discuss who can obtain privileged access to perimeter security systems.
- Should discuss the procedure to request a perimeter device configuration change and how the request is approved.
- Should discuss who is allowed to obtain information regarding the perimeter configuration and access lists.
- Should discuss review cycles for perimeter device system configurations.

There are very few valid reasons why a member outside of the security and network support staff would need access to firewall configuration information.

Perimeter device configuration information should never be stored on, or transmitted to systems of general availability, and they should almost never be printed in hardcopy form.

In a large organization, it might be useful to have all firewall configuration changes reviewed by a small group of people who are responsible for security.

Virus Protection and Prevention Policy

- Provides baseline requirements for the use of virus protection software.
- Provides guidelines for reporting and containing virus infections.
- Provides guidelines for several levels of virus risk.
- Should discuss requirements for scanning email attachments.
- Should discuss policy for the download and installation of public domain software.

Example Text:

All <Company Name> PC-based lab computers must have <Company Name>'s standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Department managers are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into <Company Name>'s networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.

Refer to <Company Name>'s *Anti-Virus Recommended Processes* to help prevent virus problems.

Noted exceptions: Machines with operating systems other than those based on Microsoft products are excepted at the current time.

Virus Protection and Prevention Policy

- Should discuss frequency of virus data file updates.
- Should discuss testing procedures for installation of new software.

This page left intentionally blank.

Password Policy

- Provides guidelines for how user level and system level passwords are managed and changed.
- Discusses password construction rules.
- Provides guidelines for how passwords are protected from disclosure.
- Discusses application development guidelines for when passwords are needed.
- Discusses the use of SNMP community strings and pass-phrases.

As a minimum, you should have a password management policy or procedure which describes how often passwords are changed and how you track who has what passwords.

Example text:
All system-level passwords (e.g. root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

All production system-level passwords must be part of the InfoSec administered global password management database.

All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.

User accounts which have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

Other Important Policies

- A policy which addresses forwarding of email to offsite addresses.
- A policy which addresses wireless networks.
- A policy which addresses baseline lab security standards.
- A policy which addresses baseline router configuration parameters.
- A policy which addresses requirements for installing devices on a dirty network.

These are just a few examples of the types of policies that may apply to different organization. The policy development area is certainly one area where "one size does not fit all." The culture of the organization will have large impact on the types of policies that are implemented and how they are enforced.

Security Procedures

- Policies only define "what" is to be protected. Procedures define "how" to protect resources and are the mechanisms to enforce policy.
- Procedures define detailed actions to take for specific incidents.
- Procedures provide a quick reference in times of crisis.
- Procedures help eliminate the problem of a single point of failure (e.g., an employee suddenly leaves or is unavailable in a time of crisis).

Procedures are equally important as policies. Often the polices define what is to be protected and what are the ground rules. The procedures outline how to protect the resources or how to carry out the policies. For example, a Password Policy would outline password construction rules, rules on how to protect your password and how often to change them. The Password Management Procedure would outline the process to create new passwords, distribute them as well as the process for ensuring the passwords have changed on critical devices. There will not always be a one-to-one relationship between policy and procedures.

In the next few pages we will review just a few of the important procedures that almost every organizatio needs.

Configuration Management Procedure

- Defines how new hardware/software is tested and installed.
- Defines how hardware/software changes are documented.
- Defines who must be informed when hardware and software changes occur.
- Defines who has authority to make hardware and software configuration changes.

The configuration management procedure would typically be defined at the department level or at the corporate level. Even if there is a corporate CM procedure, individual groups may choose to have their own. The CM procedure should define the process to document and request configuration changes of all scales (from a simple router installation to a major firewall ACL change). Ideally, there is a central group that review and approves of all change requests. A CM process is important for several key reasons:

•Documents changes made. Provides an audit trail

•Documents that possible system down-time so that when the change is made it is not seen as a system problem.

•Provides a way to coordinate changes so that one change does not severely impact another change.

Data Backup and Off-site Storage Procedures

- Defines which file systems are backed up.
- Defines how often backups are performed.
- Defines how often storage media is rotated.
- Defines how often backups are stored off-site.
- Defines how storage media is labeled and documented.

The backup and off-site storage policy may be required due to customer commitments. The number of people who can request off-site backup tapes should be kept to a minimum. You should try restoring from backup media on a regular basis to test integrity of backup methods. Part of the backup procedure may be in the form of a program or script which automates the process of performing backups.

Incident Handling Procedure

- Defines how to handle anomaly investigation and intruder attacks.
- Defines areas of responsibilities for members of the response team.
- Defines what information to record and track.
- Defines who to notify and when.
- Defines who can release information and the procedure for releasing the information.
- Defines how a follow-up analysis should be performed and who will participate.

A incident handling procedure is a definite must for all organizations.

It is impossible to outline responses for all incidents, but you should cover the major types of incidents that might occur. Some example types might include: network port scan, denial of service attack, compromised host, compromised account, and inappropriate use.

You should identify one person to act as a liaison to outside agencies.

Policy Resources

- RFC2196 - The site security procedures handbook
  - Obsoletes rfc1244 as of 09/1997
  - *http://www.ietf.org/rfc/rfc2196.txt?Number=2196*
- Some useful web sites:
  - *http://www.gatech.edu/itis/policy/usage/contents.html*
  - *http://csrc.nist.gov/isptg/*

It is difficult to find general resources for business oriented policies. Many companies consider their security policies to be sensitive information.

Recap

- Policies are a crucial part of the infrastructure.
- Trust is frequently an issue.
- Key policies:
  - acceptable use policy - remote access policy
  - information protection policy
  - perimeter security management policy
- Key procedures:
  - CM procedure
  - incident handling procedure

This page left intentionally blank.

