Global Information Assurance Certification Paper

Creating Security Policies – Lessons Learned

Mark Worthington

May 4, 2001

Introduction

One of the core principles in Information Security is adherence to the organization's security policy. After attending SANS training or other security classes we return to work with an eagerness to move forward with hardening servers, tightening firewalls, and implementing intrusion detection systems. As our first step, of course, we identify our need to comply with the existing security policy. So we begin our search to see if we even *have* a security policy, and end up dusting off an old notebook we found on a shelf somewhere. What we find may not even be applicable to our current environment, is so generic that it's woefully incomplete, or has become totally out of date. What do we do next? This paper shows the reader some steps we have taken on our continuing journey towards a full set of security policies and procedures.

Revising the Policy

What do we do if the current security policy is incomplete or out of date? In our case I spoke with my Director and shared the vision with her of how important it was to update our current Electronic Use Policy. She was quite receptive, already being familiar with the critical role played by such a document. It was clear that the current Electronic Use Policy would need to be significantly revised and enhanced to cover acceptable use of resources, greater levels of security awareness, and increased user involvement.

We needed to expand the scope of what the current policy covered, and to ensure that all 2500 employees knew what was in it. To accomplish that we would have to find an effective way to educate each person, and to verify that everyone knew what was expected of them in maintaining compliance. Rewriting the policy to cover every identified vulnerability, publishing it to users, and testing for compliance seemed to present quite a daunting task, when what we really wanted to do was to get started making our environment more secure. Where do we start?

As it turned out we were able to begin working both issues concurrently. Implementing several server fixes would not violate any current policy, so we were able to begin hardening certain aspects of our enterprise even as we started updating our documentation.

The Approach

Since the previous security policy didn't address as broad a scope as what we need now, we decided to temporarily set aside the older document and begin to produce a new one. Information Systems had been charged with developing the original policy years earlier, so after speaking with the Legal Department and Human Resources I simply began to write what came to mind. This became something of a free-form brain dump of concepts

and ideas learned in the SANS Security Essentials curriculum and elsewhere. After a few rounds of this core dump I went back and began to refine the sections and wording. As time allowed I added to and modified different portions of the document, but was unable to devote full attention to it while balancing urgent work on all our other active projects.

An observation here: Whereas security policies must address the three foundational concepts of ensuring confidentiality, integrity, and availability, they are also designed to create end user awareness and participation. With this in mind it is logical to include other related matters in which we need user education. As we work through the process of creating security policies we will also focus on areas that may not seem to affect the "big three" security aspects directly, but are very important for the overall health of the organization. These will include acceptable use policies for the equipment, data, email, Internet, and others as needed. As we will see in a moment these can cause significant liability problems if not handled carefully, and do fit in naturally with an instructional program on password selection, use of non-approved software, and social engineering.

During the writing process I was eventually able to go back and directly consult the SANS coursework[1] where we find eight important topics that should be included in a good security policy.

- **Purpose** – the reason and goals for the document
- **Related Documents** – citing other pertinent policies and procedures. These could include specific instructions for server administrators, network auditors, or end users. The policy paper I started writing tended to mix procedures in with the policies; those should be moved to other referenced documents before the policy is complete and ready to be reviewed, signed, and implemented.
- **Cancellation** – describing which documents this supercedes
- **Background** – a reflection on the need for security policies
- **Scope** – the range of issues covered and to whom they apply
- **Policy Statement** – SANS' description says, "the statements should define actions that are prudent, expedient, or advantageous to the organization."[2] The policies must be realistic. It doesn't help to declare that no personal use of computers will be allowed if that is not something that will be enforced. An article from ComputerWorld as quoted by CNN states
    - "Dallas attorney B. J. Thomas, who specializes in computer law, said that, as counsel for the city of Cleveland, Texas, her rule of thumb is that e-mail is a tool like any other. 'Any policy can be violated by the use of another tool as well,' Thomas said. 'In municipal law, [the idea is]: Don't have a policy unless you can enforce it, and if you enforce it, enforce it uniformly.'"[3]

  An organization would probably be better off leaving out statements prohibiting personal use of email or Internet entirely if no one is expected to live by them, rather than to undermine the user community buy-in of the entire security policy. The policy also may not be legally enforceable due to inconsistent application of it, should a serious violation of some other section occur. Again, think things through carefully and be realistic.

- **Responsibility** – identifies which people are responsible for the various affected areas within the policy. Examples include the CIO, system administrators, and attorneys. It can also define the need to create specific procedures for implementation and enforcement of the policies, referencing the **Related Documents** mentioned above.
- **Action** – specifies the tasks to be done, and the timeframe in which they are to occur.

Some of these sections I had included, and others need to be added still. It is definitely a work in progress.

For further input I consulted an excellent book by Michael R. Overly called **e-policy** How to Develop Computer, E-Mail, and Internet Guidelines to Protect Your Company and Its Assets[4]. Mr. Overly very concisely covers numerous important issues. One suggestion is that the policy should state that "personal" computers and the data stored on them actually belong to the company, and that employees do not have an assumed right to expect privacy in what they create on the computer or send through an email system.[5] The policy also needs to explain that the organization will be regularly or randomly monitoring network activity, including email, and that the purpose of users having secret passwords is not for their privacy, but to provide security for the company's data. He even emphasizes the importance of maintaining the corporate culture in a way that does not belie what is expressly stated in the policy.[6] In other words, if staff members or management speak or act in ways that suggest their computer work or emails are private it may weaken the company's position if someone were to file an invasion of privacy lawsuit. By explicitly stating in the policy that the organization has the right to monitor emails and other network traffic, and not undermining that understanding through subsequent actions, an organization should be able to avoid privacy disputes.

In the creation of all policy documents be sure to consult your attorney, the user community, human resources department, and perhaps the local bargaining unit as advised. Also, please understand that this paper in no way should be construed as providing legal advice or covering every pertinent issue.

Proactive Monitoring

In addition to privacy issues, there is also the matter of "harmful material" entering the workplace. Items such as pornography or jokes in poor taste can create a hostile work environment.[7] If someone in the office becomes offended by something they see or hear as a result of someone else's email or Internet experience they may file a harassment lawsuit against the company.[8] Filtering programs, from companies such as Surfcontrol[9] and Websense[10], are available to block URL's, or to monitor for combinations of words and phrasings within email traffic itself that might indicate offensive jokes and stories.

The usage of email is an entire issue in itself. There are many ways email can be used to cause a company great distress in the event of a lawsuit, or can force expensive discovery

processes to reconstruct an electronic "paper trail." Well-written policies covering email classifications and retention are becoming extremely advisable. Attorney Jim Bruce is quoted by Infoworld on cnn.com as saying "'If a company is sued, it is routine for the other party to ask the company to produce all their records [on the subject], including e-mail,' Bruce says. 'E-mail is a really juicy target because it can be searched by keyword."'[11]

Network and email filtering and monitoring technologies can be a very significant investment in time, hardware, software, and recurring maintenance costs for URL and other updates, but it is probably worth the expense. Compared to the potential legal liability for failing to ensure a harassment-free workplace it will likely be a bargain well worth the cost.

The Downside

Using hardware and software filtering tools are good techniques a company can employ to protect its workers and itself, but there is further caution. If a company has such systems in place, but fails to act promptly and fairly on violations to the acceptable use policy, the organization can be held liable for failing to perform due diligence to remedy the situation. In other words, if you don't respond quickly enough to document and enforce appropriate discipline for any violations you may still be held liable.[12] It becomes, then, extremely important to properly implement and execute the policies and procedures in a way that provides maximum effect. This also emphasizes the importance of an organization adequately funding such an effort, including the on-going costs for personnel and their training in support of these tools.

Whew! The more I studied on the topic of policies and their legal ramifications, the more I realized I had no desire to continue writing the stinkin' things. I really just wanted to make the operating systems and network more secure.

Another Option

Somewhat overwhelmed and discouraged I set this project aside and resumed my other daily tasks, which of course includes reviewing security bulletins. In a recent release of the SANS Newsbites[13] I found an ad declaring "Write Your Information Security Policies in a Day!" Hoping for the best I decided to contact Pentasafe[14] to see what they had to offer. I was very impressed.

The link referenced in the Newsbites article[15] took me to a page introducing Pentasafe's VigilEnt Policy Center (VPC), which then led to subsequent links[16] describing key features and benefits. The product apparently comes with pre-built security templates written by Charles Cresson Wood, an expert in the security field, and which are accessible through a wizard application that steps you through the policy creation

process. According to their statements you can have a draft security policy prepared in about a day. That sounds good to me.

A quick note: This paper is not intended to be a product review, but was created to share with the reader some of the steps and thought processes our organization is going through to update our security policies. I hold no stake in Pentasafe, and have not even seen a demonstration of VPC yet. I have requested one from the vendor and am looking forward to determining if this product will help simplify our task. If VPC works as well as claimed I plan to consider incorporating it into our environment, provided funding becomes available. We have a significant budget process to work through, so this may not be feasible right away. As I share with the reader some additional features claimed for this product, it should become apparent how they might prove helpful in the enterprise.

Publishing the Policies

In addition to creating and editing security policies there must be an effective mechanism to distribute them to the user community. As mentioned earlier, we might have in place the best policies in the world, but if our users don't know what they are, and how that impacts the way they perform their jobs, it will do little good towards accomplishing the goal of keeping our networks and data secure. User education is imperative, as is the ability to verify that everyone understands and has agreed to abide by the policies and practices. PentaSafe's VPC seems to provide a good solution to educate, test, and catalog user awareness.

According to the documentation VPC allows administrators, once they have worked through the automated policy creation process, to publish the finished documents to a company's intranet site. Rather than just hoping users will visit, read dozens of pages, and thereby become fully supportive, VPC goes further. The product is stated to provide a quiz mechanism to test and record user participation in the on-line policy training program. Users log in at their convenience, or with prompting, and are then educated and tested on their knowledge of the company's policies. A permanent record of their participation is stored, and remains available should an incident of violation arise later. Employees are protected by always having on-line access to the company's policies in case they have questions, and the company is protected by being able to prove that it has performed due diligence in crafting policies and educating employees. It is Win-Win.

Summary

PentaSafe's VPC is certainly not the only method available for an organization to develop and implement security policies and procedures. It is entirely possible for a company to create its own policies from scratch, or to copy and paste some boiler-plate wording that might be provided by others as a service on the Internet. However, allocating sufficient internal staff time might not be a cost-effective option, especially considering the potential legal liability that is at stake. The proper skill set mix of writers, attorneys, human resource specialists, technology experts, etc., may not even be

available within local staff. Outsourcing a portion or the entire job may be an option for some. It is, of course, ultimately up to each organization to determine their best course of action to fill this essential need.

Conclusion

As I noted at the beginning of this paper I was hoping to share with the reader some lessons we have learned. Perhaps trying to write all the policies and procedures ourselves is not the best way to go, hence our current interest in exploring VPC. We are not yet finished creating our documents, so we are actually still in the thick of it with you. It would have been nice to be on the other side, encouraging your progress along a well-worn trail. I wish we had the definitive words of wisdom for others heading down this path, but perhaps some of the issues discussed will help you explore a few options and to determine what works best for you.

Appendix A

As a reference I have included the text of our current work-in-progress. Be aware that this is only a draft document and in need of revision and review. Hopefully some ideas will stimulate your own thinking.

Acceptable Use Policy
Security Policies and Procedures for <ORGANIZATION>

Background

The <ORGANIZATION> has set a vision and is progressing on a path into the future of enhanced constituent support and service by maintaining a secure and available network of electronic data systems. These systems are interconnected via high-speed switches, routers, and firewalls to allow appropriate access to <ORGANIZATION> information stored on multiple file servers and databases. The goal is to maintain all of these components, along with the backup devices and supported client PCs, in a manner consistent with industry best practices.

Contained in this document are the policies that direct the processes and procedures by which <OUTSOURCING VENDOR>, in partnership with the <ORGANIZATION>, strives to maintain a secure and available data enterprise. By employing industry best practices along with proprietary processes we are working to provide due diligence in our best efforts to maintain the confidentiality, integrity, and availability of the <ORGANIZATION>'s data resources.

This endeavor is truly a partnership, in that all parties involved have a significant stake and responsibility to comply with all agreed-upon policies and procedures to ensure the highest possible level of security. A single weak link anywhere in the chain, from the largest server, to any individual user running an unauthorized program, could compromise the integrity of confidential data or create a catastrophic loss. There are "hostile" applications that can inadvertently or deliberately be run on a PC and cause data destruction or disruption of service to others. Information Systems is constantly working to harden systems against such attacks, and to implement services to screen out hostile mobile code and viruses, but it is still up to each individual user to comply with all revisions of published policies and procedures. Risk assumed by one is shared by all.

The latest version of the <ORGANIZATION>'s Acceptable Use Policy will always be posted on the <ORGANIZATION>'s Intranet site for quick reference.

As all <ORGANIZATION> network users carefully follow operational and security guidelines we have a good opportunity to continue providing the best possible services to the employees, residents, and businesses of the <ORGANIZATION>.

Scope

This document contains multiple sections that are in many ways inter-related. Several concepts, with Security being foremost, become threads that run through the entire document and are common to multiple areas of discipline. The overall objective, of course, is to guard the <ORGANIZATION>'s vital electronic data resources that contain confidential employee records, payroll information, customer information, and much more. All of these records are stored in electronic data systems and must be treated in a manner consistent with current best practices to ensure their confidentiality, integrity, and availability.

This document strives to define methodologies to support the three essential principles for guarding electronic data systems:

- **Confidentiality**
- **Integrity**
- **Availability**

Briefly describing each quality we have

Confidentiality – Ensuring that only authorized users can access confidential or sensitive information. By precisely defining groups of users, and regularly auditing the accuracy and consistency of those groups, we can limit and control who has access to which data. Through a variety of policies, practices, and systems we work to ensure that only those who are authorized will access any given data resource.

Integrity – Ensuring that data has not been tampered with, either on the network or in storage. Our goal is to ensure that data integrity is maintained at all levels.

Availability – Data must be available to those who are authorized to use it. Denial-of-Service attacks are becoming common, and our goal is to ensure that users can access the data they need.

Target Audience

The policies and procedures described in this document cover various groups of people. Some policies cover every user of the <ORGANIZATION>'s network and its resources, and others apply to specific groups who administer or manage the network. This is not discriminatory, it is simply a function of roles and responsibilities. The identified groups are listed below.

- <ORGANIZATION> Employees
- <OUTSOURCING VENDOR> Employees
- <ORGANIZATION> Information Systems staff
    - Includes both <OUTSOURCING VENDOR> and <ORGANIZATION> Employees
    - Managers
    - Network Resources Division
    - Server Support Division
    - Desktop Support Division
    - Data Center Operations Division
    - Network Security Division

- Each and every individual person who uses any portion of the network or its resources

Ownership of Network, PC, and Data Resources

All hardware and software are the property of the <ORGANIZATION>. Although there are numerous "Personal Computers" provided for use by staff members they are owned by, are to be used for conducting business for, the <ORGANIZATION>.

Hardware

Any computer or networking hardware must be approved through the formal Information Systems approval process before being connected anywhere on the network.

Software

No software may be loaded on or removed from any <ORGANIZATION> computer unless it has been approved through the formal Information Systems approval process.

Usage of Network, PC, and Data Resources

Any person using the <ORGANIZATION> computer network or any of its components must agree to and abide by all parts of the Acceptable Use Policy.

No Privacy of Data
Detail here.

Privacy Rights Waiver
Detail here.

Computer Usage Monitoring
Detail here.

Network and/or email Monitoring
Detail here.

Allowable Use of Computer Systems
Detail here.

Formal Information Systems Approval Process

Defined and explained here.

Security

Security must be an integral thread running through every aspect of the enterprise. Just as physical security for employees has been provided with policies, guards, and metal detectors we must also provide for security of the <ORGANIZATION>'s data using a multi-layered approach.

Each PC user is entirely responsible for his or her own user ID and password. No one else should share these. Every file server and piece of networking equipment has its own mechanisms of protection through access codes as well.

Security is everyone's business, and is an on-going refinement process as situations change and new vulnerabilities develop. This section discusses several aspects that should be universally applied in addition to any other, more specific, policies that are developed.

Several other sections within this document will address security again as it applies to specific areas.

UserID's and Passwords

Individual user accounts and passwords are used to create security for the systems and data belonging to the <ORGANIZATION>. As mentioned earlier, users should have no expectation that anything they create, store, send, or receive on a computer or through the network is private; all data is the property of the <ORGANIZATION> and is subject to review at any time by authorized personnel. The purpose of a UserID and password is to create security from unauthorized access to the <ORGANIZATION>'s systems or confidential data.

UserID Creation

The <ORGANIZATION> has a standard method for creating login names to servers, applications, databases, and email. The UserID consists of 8 characters. The first character is the same as that of the user's first name. Appended next is that portion of the user's last name that will fit within the 8 character field. If the last name is too long, it is truncated at syllable breaks to fit.

Since all UserIDs must be unique throughout the <ORGANIZATION> there will be instances where a "tiebreaker" must be used to keep similar names from resulting in the same 8 character value. We will insert a new character into the second position to create unique ID's.

For example, if Mary Smith already has MSMITH and Marvin needs to be added, we will create his UserID as MASMITH. When Mellisa Smitherington is added later her UserID will become MBSMITH, and so on. By sequencing letters of the alphabet we are able to accommodate numerous such situations.

Password Length and Complexity

Most user ID's have been assigned by a system administrator to be used for each individual person to log into the network. In addition, there may exist other ID's for users to access specific databases or applications. It is permissible to use the same password for each system or application a user accesses.

In all cases each user is entirely and personally responsible to maintain the complexity and secrecy of his or her own password.

All passwords must consist of

- At least 8 characters
- A combination of uppercase and lowercase letters
- Numbers
- Special symbols (~!@#, and so on).

Remember, each password should have all of the above in it.

Please, it is important NOT to use

- Your login name
- Your dog or cat's name
- Anyone's birthday
- Any single word found in any dictionary in any language

Yes, this sounds difficult, but any of the above passwords are easy to guess or crack by an attacker trying to access the system. Even if you think you don't have access rights to anything important, you must still protect the secrecy and complexity of your password. If an attacker can get in using your account, he has a foot in the door and may be able to break further into the network.

How then do you select a password that you don't have to write down on a sticky note and attach to your monitor? (Please don't ever do something like that! You might be surprised, but that is a very common way attackers get into systems.)

Remember, you must safeguard your password at all times, so if you need to write it down, put it into your wallet or purse where you keep your other valuables like a drivers license or credit card.

Do you think you could come up with or remember a password that fits those requirements? How about the one here?

Il2satMoA!

It looks very difficult, but if you are told that it stands for "I love 2 shop at the Mall of America!" you won't have any trouble remembering it. This is called a pass-phrase, and it helps to create a very complex password that is quite secure. Again, write it down but only store it with your valuables and don't leave it lying around. Also, please don't use this example since it has been shown here.

Password Secrecy

Under normal circumstances no password is to be shared between people. If an instance arises where someone must log into a system to access another's files, the owner of the login may share the password on a short, temporary basis to complete the needed work. At the earliest possible convenience the owner must create a new password, something unknown to others. If there is a reason for one person to access another's files for longer than a few days, you should contact the helpdesk to request a change of access rights for your account.

Remember, you are entirely and solely responsible for any loss, damage, or misuse of data that may occur by anyone who logs on with your UserID and password. Keep your UserID, and especially your password secret.

Persons Exempt from the Password Policy

No one! Some people find password policies annoying and inconvenient, but how embarrassing or damaging to the <ORGANIZATION> would it be if the CEO or CTO's PC and network accounts were hacked into and damage caused due to a weak password. Let's all work together to ensure the security of the entire network.

Password Rotation

Passwords must be changed regularly to avoid the possibility of them eventually being discovered and compromised. Therefore, each user must change his or her password at least once every six months. The password may be changed more often, but you can not reuse the same password within a three-month period.

Forgotten or Temporary Password Assignments

Occasionally a user may forget his or her password. When that occurs they are to call the helpdesk to request that a new, temporary password be assigned. Helpdesk will comply by scheduling or having a technician put in a new short-term password. Neither the helpdesk person nor the technician is permitted to divulge the new password to the person calling. They must both hang up; helpdesk will look up the user's name in the <ORGANIZATION> employee phone directory. They will then call that number and leave the new password on voicemail after hearing the intended person's recorded message. By taking this small extra step it will help to reduce the likelihood that an attacker could successfully obtain a login by impersonating a valid user.

Password Cracking

Part of maintaining a security policy is ensuring that there are no weaknesses caused by failure of some users to follow policies and procedures. There will be times when certain Information Systems personnel

will test, or hire others to test, various portions of our enterprise to verify overall security. One test will use common tools to ensure that passwords are maintained with sufficient length and complexity as stated in the password policy. We will deliberately and purposefully run tests in a manner that will avoid cracking passwords that are crafted properly. Passwords that do not meet ALL of the requirements will most likely be discovered during this process.

This practice ensures privacy of data for the users who are helping contribute to the overall security of the <ORGANIZATION>'s resources by following security policies. Those users whose passwords do not meet the proper standards will be notified by email to correct the situation.

It is expressly against policy for anyone to run any type of password cracking tool or network penetration testing without proper authorization. Only certain specific persons who have proper documents on file with the <ORGANIZATION> Manager's office are permitted to initiate or permit such activities. Disciplinary measures will be taken against those who violate this policy.

Network Infrastructure

Background

Routers, switches, firewalls, as well as various Unix and NT servers, comprise vital services that make possible the <ORGANIZATION>'s extensive data network. Management of these components is delegated to different groups, but they all must work together in a secure, stable, and managed way to provide an effective network. Because some of these components exist in the more vulnerable perimeters of the network they necessarily must be hardened and configured appropriately.

Network Components

These components include

- Routers
- Switches
- Firewalls
- DNS Servers
- Proxy Servers
- Web Servers
- FTP Servers

Network Component Passwords

Network components must be configured with passwords of the same type and complexity as described elsewhere in this document. Due to the critical nature of their functions they must be subject to more stringent policies, and therefore the passwords are managed as follows.

In keeping with the maxim to provide defense in depth, each infrastructure component located in or supporting the perimeter networks must have a unique password. In other words, the external Internet router, firewall, proxy servers, mail servers, DNS servers, FTP servers, and all other DMZ servers must have passwords totally different from each other and from all others anywhere in the network. The reasoning behind this is that if an attacker is able to penetrate one level of security he will have to start over at each new device, not having captured "the keys to the kingdom" after acquiring and cracking one system's password file. For the same reason, only one or two critical administrator accounts, also with unique passwords, should ever be stored on a system in the perimeter network.

Network Component Passwords – Contingency Access

Two sealed envelopes containing passwords are to be stored in a locked box in the office of the Information Systems Director. One envelope will contain the logins and passwords for all routers, switches, and CSU/DSU's maintained by Information Systems. The other envelope will contain the passwords for the Unix servers and all databases. In the event that the appropriate Network Support or Server Administrators are not available in an emergency access to the secured envelopes can be provided by one of the following people:

John Smith – Information Systems Director
Mary Jones – Departmental Accountant
Judy Doe – Administrative Assistant

Network Component Passwords – Change Cycle
Passwords on infrastructure components must be changed at the following times.

- At least once every three months
- In the event that a password or system becomes compromised all infrastructure passwords are to be changed as soon as possible
- In the event that the sealed envelopes containing the passwords secured in the Director's office is opened for any reason the passwords are to be changed

Prior to any passwords being changed, a new sealed envelope containing the new passwords will be placed in the designated storage area in the I.S. Director's office. The effective date of the new passwords is to be written on the outside of the envelope, along with the names of the supported equipment. Both the old and new envelopes are to be retained in the locked box until the next round of password changes, or until the next Security Audit Reporting Cycle occurs, whichever comes first. This will cover the unlikely contingency that one or more of the devices is overlooked in the password change process.

Network Component Passwords -- Assignment and Responsibilities
Routers and LAN Switches
All routers and LAN switches are maintained and supported by the Network Services group of Information Systems. Login passwords and privilege-level passwords are assigned and retained as confidential by two support persons.

Bob – Network Services Manager
Fred – Network Engineer

Public Safety DSU/CSU's
All DSU/CSU's are maintained and supported by the Network Services group of Information Systems. Login passwords and privilege-level passwords are assigned and retained as confidential by three support persons.

Bob – Network Services Manager
Fred – Network Engineer
Marvin – VAX Support Technician

Network Infrastructure Support Servers
All Unix servers are administered by the Data Center Management Group. Root passwords are assigned and retained as confidential by three support persons:

Oscar – Data Center Manager
Ralph – Senior Systems Administrator
John – Unix Systems Administrator

Servers

Background
All network operating systems are subject to problems that don't become evident until they have been in common use for some time. Manufacturers periodically release service packs and patches to repair what has been found. Additionally, there are services and features that may be useful in certain, low risk environments, but for the majority of installations they create unreasonable security and operational risks. As various vulnerabilities are discovered by users and specialists in the networking field recommendations are made to make adjustments to operating systems to alleviate these problems.

New Server Prerequisites

In light of the need for remediation of identified problems, and the severe security risks posed by ignoring them, no server will be permitted to be connected to the <ORGANIZATION>'s operational network until it has been sufficiently hardened.

Procedures will be defined for each unique operating system to identify, document, and implement current best practices for each platform, to include, minimally, Microsoft Windows NT, Windows 2000, Novell, Unix, and Linux. These procedures will probably be the most dynamically updated, as vulnerabilities are announced almost daily. Sources from which these procedures will be drawn are the vendors themselves, the SANS institute, and other reliable sources.

Production Server Patch Maintenance

A policy and procedure will be developed to allow quick dissemination of the current best practices for servers to ensure the production systems are kept in top condition. However, no patch or fix will be applied to any production system until it has been carefully tested on the development servers to ensure that the "cure" isn't worse than the disease.

Workstations

New Workstations

Because the <ORGANIZATION> standard for PC desktop operating systems is Windows NT Workstation they are subject to most of the same vulnerabilities experienced by NT Server. Therefore, all new workstations must be subject to the same policies and procedures as the servers to harden them. In addition, there are many applications and PC settings that can cause weaknesses in the integrity of the desktop, and even other systems on the <ORGANIZATION> network.

To create uniformity of setup and to ensure that known weaknesses have been resolved it will be necessary to create a standardized image of PC desktops. It is expected that Novell Zenworks will be employed to help the imaging and deployment of standardized setups.

…..

Backup Systems

……

Tape Rotation Schemes

Off Site Tape Storage

P & P's for encrypting data on tapes going offsite

P & P's for Tape Backups performed on Off-Site Servers

P & P's for Tape Backups performed by Non-supported groups

Tape Integrity and Usability Testing

It does no good to run regular backups if valid, useable data is not actually stored on the tapes. Therefore, Backup Policy requires that backup log files are checked daily. In addition, periodic testing will be done to ensure that a complete system and data restoration can be done. Spare servers will be made available by the <ORGANIZATION> to make this essential step possible.

References:

[1] SANS Institute, The. "Basic Policy." Track 1: Security Essentials Book 1.1. Version 1.35 (2000): pp. 5-12 and 5-13.
[2] Op. cit.
[3] Disabatino, Jennifer. "E-mail probe triggers firings." Computerworld. 11 July, 2000. URL: http://www.cnn.com/2000/TECH/computing/07/11/email.firing.idg/index.html
[4] Overly, Michael R. **e-policy** How to Develop Computer, E-Mail, and Internet Guidelines to Protect Your Company and Its Assets New York: SciTech Publishing, Inc, 1999.
[5] Op. cit. 26.
[6] Op. cit. 27.
[7] Trombly, Maria. "Dow to fire up to 40 employees over sexually explicit e-mails." Computerworld. 24 August, 2000. URL: http://www.cnn.com/2000/TECH/computing/08/24/dow.sex.firing.idg/index.html
[8] "If A Supervisor Engages In Harassment, Is The Employer Ultimately Responsible?" URL: http://employment-law.freeadvice.com/sexual_harassment/supevisor_employer.htm
[9] Surfcontrol plc. http://www.surfcontrol.com/
[10] Websense Inc. http://www.websense.com/
[11] Steen, Margaret. "The legal traps of e-mail." Infoworld. 6 July, 1999. URL: http://www.cnn.com/TECH/computing/9907/06/emailtrap.idg/index.html
[12] Overly, Michael R. **e-policy** How to Develop Computer, E-Mail, and Internet Guidelines to Protect Your Company and Its Assets New York: SciTech Publishing, Inc, 1999. 36.
[13] SANS Institute, The. "SANS Newsbites Vol. 3 Num. 18." 2 May, 2001.
[14] PentaSafe Security Technologies, Inc. http://www.pentasafe.com/
[15] http://www.pentasafe.com/products/policyoverview.htm
[16] http://www.pentasafe.com/products/vspm.htm

Last Updated: September 25th, 2017

Upcoming Training

Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event