Global Information Assurance Certification Paper

Submitted By: Rob Doolittle
GSEC Practical Assignment Version 1.2f
Title: Policy Without Consequence

Policy Without Consequence
One Companies Network Security Policy Document

Introduction

In this paper I will discuss the computer security policy document I drafted for XYZ Inc. a pharmaceutical research company. I would like to explain some of our company's policies and procedures that help us achieve our computer security goals. For good policies to be effective, it is important to monitor those policies in several ways. Do the policies reflect the current business model? Do our employees understand them? Are the policies doing the job we intended them to do? The policy document should be adaptable as a business grows and embraces new technologies. A security policy document is a living document, and should be reviewed and revised on a regular basis or as the need for change becomes evident.

Ensure a sound "security culture"[1]

For security measures and policies to be effective, we must develop a sound "security culture"[1]. To be effective this "culture" must have the full support of senior management, employee awareness, employee training and be implemented in a way as not to prohibit the work of our employees. Senior management should act as role models and demonstrate a positive attitude towards the security policies developed.

All employees are required to read and sign the Computer network Policy Document. This document is presented at time of orientation. Not only is the employee required to read the document, each topic is discussed. The employee is encouraged to ask questions to clarify any points they do not understand. In addition to the Computer network Policy Document, new employees are required to view a presentation concerning corporate security, which covers such topics as electronic devices and physical access security policies. Only after this document has been signed, is a computer account established for the individual. Below are the regulations addressed in the document.

"Components" of The Computer network Policy Document

1. Access to the computer network will require both your login name and your password. Your password is to be used by you and only by you. You shall not give your password to any other person for any reason. Memorize your password. Your login name and password combination serves as your electronic signature. Actions taken under your login name and password carry the same validity as your hand written signature. Making your password available to any other individual will result in immediate termination.

2. Your password is case sensitive and must be entered for login exactly as you registered it. Your password must be at least seven characters, contain letters (both upper and lower case) and numbers. In addition you may use special characters. Do NOT use any of the following for your password selection: license plate number, social security number, birth dates, names of friends, family or pet's. Easily

guessable combinations (example: abc1234) should not be used. Passwords will expire every 90 days. When your password expires you will be prompted to enter a new password. You may not reuse your current password.

3. If you leave your computer for any period of time, you are required to save your work, exit all programs and logout. You may also lock your workstation. At the end each day you should exit all programs, shut down and turn off the power to your workstation.

4. Emergency and critical situations involving a computer system's operational capacities are not to be made public. Clients and/or visitors are not to be made aware of any such situation. This information is considered confidential. Failure to comply with this policy could result in termination.

5. In the event that a computer virus may be exposed, that information is considered confidential and must not be made public or disclosed to clients and/or visitors. Non-employees and others outside the company are not privy to corporate responses and announcements of such activity. Notification to non-employees or the forwarding of corporate e-mail external to the company regarding these instances could result in termination.

6. Employees are not permitted to install their own software (including screen savers) or download programs from the Internet without the consent of the Network Administrator. Only authorized programs may reside on corporate computers. Should an unauthorized program be found on any company computer, the responsible party may be charged for the removal of that program and any reconfiguration that may result.

7. The deliberate introduction of a computer virus into the system or any other malicious action, physical or technical, against any XYZ Inc. computer and/or electronic based system(s) will result in termination and criminal prosecution to the fullest extent of the law.

8. Corporate issue or personally owned computers used to remotely access any XYZ Inc. network must have currently approved anti-virus software installed and activated. The company will provide and install this software.

9. The use of password crackers, port scanners, or any like programs and/or device used to deliberately breech system security will result in immediate termination and criminal prosecution.

10. The use of the Internet for the purpose of engaging in illegal activities and/or the viewing and/or posting of sexually explicit and/or hate-related materials will result in termination and possible criminal prosecution. Acceptable Internet activity is that which enables you to complete your duties as set forth in your job description, not detract from your professional productivity, and that which is not offensive to others.

11. Employees will not engage in any form of work, consulting, or assistance using XYZ Inc. computer systems for any entity or person other than XYZ Inc.

12. XYZ Inc. reserves the right to inspect all computers and computer related equipment. All files, documents, data, e-mail, and programs are considered company property. There is no privacy on company computers. Your electronic actions may be monitored or tracked.

13. Your signature on this document states that you understand and will follow the policies and regulations described above.

Let's take a closer look at several regulations addressed in the Computer network Policy Document.

Number one: Passwords are only as good as the people who possess them. They can be given to someone else; they can be written on a Post-It or worse, written on the underside of a keyboard. In the pharmaceutical environment, electronic signatures and logins are equally important for maintaining a valid audit trail in our analytical systems. We place an enormous degree of significance on their proper use. People seem to be the weakest link in the security model. However, with the proper training on acceptable use, and making employees aware of the importance of security, this risk can be minimized.

Number two pertains to password format. We do enforce the use of strong passwords. Passwords expire after ninety days. The system remembers the last ten and you cannot reuse them. Accounts are locked after three unsuccessful attempts and require administrative privilege to unlock them. Passfilt has been implemented however it does not restrict an individual from using combinations like "Abc1234". Because of this passwords are monitored. When weak passwords are "discovered" the individual's account is set to "change password at next login". If that individual uses another weak password (i.e. Abc1235), their account is locked and they are responsible directly to their supervisor and the Corporate Security Administrator. I'm sure you noted, "When weak passwords are discovered". Passwords are monitored through cracking. This brings our attention to item number nine:

> "The use of password crackers, port scanners, or any like programs and/or device used to deliberately breech system security will result in immediate termination and criminal prosecution."

You may be wondering how I am still employed. Not only have I violated item number nine; I have violated the very terms I drafted into our Corporate Security Policy Document.

> "Policies should be developed to address electronic devices, computer security and physical access. Disciplinary actions should be defined to address violations

of security policy. These actions should be equal for all employees. Management should not demonstrate a policy without consequence stance and take a firm position on infraction."

A "contract" signed by myself, the CIO, and President grants me permission to "implement the use of, but not limited to, password cracking applications, port scanners and other utilities required to insure the security and integrity of our network and other electronic systems".

I know you have all heard this before. Its importance cannot be stressed enough. Have an agreement in writing if you plan to conduct "security audits" that may violate the very policies that have been instituted to protect your facility. Even though you may be directly involved in the policy making process, a deliberate breach, even for the sake of auditing, could result in less than favorable circumstances.

Number Three: While it would be nice if everyone would logout every time they left their computer, even for a short time, that does not happen in the real world. Often confidential information pertaining to one client is viewable "on screen" while another client may be touring the facility. We have instituted policies to invoke a password protected screen saver after ten minutes of non-use. If you have a large number of systems to manage, the NT Policy Editor can help. These policies can be user or machine specific. We have instituted one for "acquisition" systems and another for desktop workstations.

Number Five: I often receive e-mails concerning viruses. Many of these are from employees who have in some form, heard about a virus and are "just letting me know". I always make a point of thanking them for their concern as well as giving them a little background on the virus. Luckily, the majority of these announcements turn out to be hoaxes. In most cases these notifications will usually state that the information is from a reliable source such as CNN, Microsoft or IBM. The unfortunate side to this is that this generates "panic" as well as e-mail, what I call the "e-chain letter syndrome". We consider it unacceptable for employees to forward any such e-mail to others. The last thing we want is several hundred e-mails concerning a hoax virus sent from "just about everybody"@ xyz.com. It may or may not be your corporate policy to send notifications to employees warning of known viruses and/or infected attachments. We do so on a very limited basis. XYZ Inc. spends a great deal of time and money on virus prevention, detection and eradication at the server level. In the virus arena proactive wins over reactive.

Number six concerns the installation of unauthorized software. Permissions on our NT workstations prohibit most users from performing installations. The auto run feature has been disabled and, the "run" selection has been removed from the start menu through the use of NT policies and/or registry key changes. In addition, floppy drives and CD-ROM drives have been removed or disabled in the BIOS. These measures not only prevent installation of software, it prevents employees from removing intellectual property on disk. There are a small number of administrative and senior management

personnel who are permitted access to floppy and CD-ROM drives. All media must be requested specifically for electronic deliverables. The request must include the reason for the request, exactly what information is needed, and to whom the information is destined. We document these request through our automated change control application.

Number Eight: Remote access is not an option open to all of our users. This is reserved for sales persons, some IT personnel and several senior management persons. Some use home systems while others use company issued laptops. In either case anti-Virus software is required and is provided at the company's expense.

As we address item ten, it is important to keep in mind a company can be held liable for the actions of its employees. The Internet has opened a giant doorway to corporate legal liabilities as well a worker productivity issues. Our company considers the Internet to include web browsers, e-mail, news groups, chat rooms as well as instant messaging services. Let's review number ten.

> "The use of the Internet for the purpose of engaging in illegal activities and/or the viewing and/or posting of sexually explicit and/or hate-related materials will result in termination and possible criminal prosecution. Acceptable Internet activity is that which enables you to complete your duties as set forth in your job description, not detract from your professional productivity, and that which is not offensive to others."

All employees have access to the Internet at XYZ Inc. Internet activity is monitored. XYZ Inc. is a small company that employees approximately one hundred people. Because of our relatively small number, specific content filtering software is not utilized. We do however monitor the appropriate proxy logs for connections to inappropriate sites. Violations concerning offensive sites are dealt with immediately. A number of "unacceptable" and "unproductive" URLs are blocked. Sites pertaining to auction houses and job searching are examples of these. To reinforce this policy, any access to a restricted site is redirected to a URL that displays the following message:

> "You have attempted to connect to a restricted site. Your attempt will be logged for further investigation."

Which brings us directly to number twelve. This often comes as quite a shock. No one could ever believe we would or could do this. I make sure our employees fully understand this statement. I strongly suggest you have a statement similar to this in your policy.

> "XYZ Inc. reserves the right to inspect all computers and computer related equipment. All files, documents, data, e-mail, and programs are considered company property. There is no privacy on company computers. Your electronic actions may be monitored or tracked."

Conclusion

Security policy documents are living documents. These documents must be reviewed and revised on a regular basis. Remember, a security policy is the first step in maintaining a safe and secure environment for our workers, our systems as well as our intellectual property. All those to which a security policy applies must understand the policy, the policy's importance, and the consequences that can result from non-compliance. It is important that we monitor our environments to be assured that our policies are effective. As security professionals, we have available to us the tools and applications that can help us maintain a high level of assurance. We must use these tools in an ethical manner and not abuse the very threats we are trying so hard to circumvent.

References:

Svetcov, Eric Sample Policy “Acceptable Use Of Corporate Information Technology Resources” March 27, 2000
URL: http://www.ithell.com/IT_Policies/Acceptable_Use/body_acceptable_use.html

Svetcov, Eric Sample Policy “E-Mail Acceptable Use Policy” March 15, 2000
URL: http://www.ithell.com/IT_Policies/E-Mail_Policy/e-mail_policy.html

University of Georgia “Policies on Use of Computers” Last Revised September 27, 2000
URL: http://www.uga.edu/compsec/use.html

D. Atkins, P. Buis, C. Hare, R. Kelley, C. Nachenberg, A.B. Nelson, P. Phillips, T. Ritchey, W. Steen (1996) “Internet Security Professional Reference” New Riders Publishing

1. J.G. Jumes, N.F. Cooper, P. Chamoun, T.M. Feinman (1999) “Windows NT 4.0 Security, Audit, and Control” Microsoft Press