GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

How to Develop Good Security Policies and Tips on Assessment and Enforcement

Kerry D. McConnell
SANS Security Essentials, GSEC Practical Assignment, Version 1.3

Summary
Every organization, regardless of size, should have documented security policies. Surprisingly, many organizations do not. The key word in the first sentence is "documented". Every organization has a position or policy on security, it just may not be written down anywhere. If your organization falls into this category, beware! Sooner or later, you are likely to encounter a situation where it could make all of the difference in the world if you are able or unable to produce your documented security policies.

It is not uncommon for individuals tasked with developing and maintaining these security policies to prefer visits to their dentist over taking on this effort. Where do you start? What should the policies cover? Will anybody really take the time to read them? How do you know if you have hit or missed the mark for developing good security policies? Invest the time up front to carefully develop sound policies and then identify ways to gauge their effectiveness and assess the level of compliance within your organization. Commit to spending the time and resources required to ensure that the policies are kept current and accurately reflect your company's security posture.

Introduction

Effective security policies form the foundation of your organization's entire approach to security. These policies should mirror your corporate culture and should be in harmony with your demonstrated business practices. Security policies are a living, breathing component of any successful organization. But as such, they require careful planning, development, and ongoing attention in order to be of the greatest value to your organization.

Where to Begin

If you have been given responsibility for the development or management of security policies for your organization, the task at hand could vary significantly. You could inherit a complete set of well-written, clearly understood policies that will only require that you keep them up to date. You may find that security policies already exist for your organization, but upon review discover that they are nearly ten years old. Or, you could be given a completely clean slate and asked to develop your security policies from scratch.

All but the first scenario described above can seem overwhelming. At times, it can be hard to even know where to begin. There are so many areas to be addressed that it can become a "can't see the forest for the trees" situation. However, it doesn't have to be so difficult. First of all, accept that you will not have a policy for every situation that could arise. Aim for creating broad policies that are far-reaching to address all of the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

areas that you deem critical to the security of your organization. Remember, the procedures you develop that actually allow security to happen must support your security policies.

If you feel completely lost, or think that your company doesn't have a security position, the SANS Institute recommends that you review your firewall rules as a starting point. The things that you allow or do not allow through your firewall will begin to define what your security posture really is. Finally, if you are having writer's block or simply cannot get started, select a few common areas to begin with and then move on to more complex topics. Good starting points include policies on passwords (length, composition, change frequency), Internet usage, and e-mail.

Security Policy Development
The following section lists additional things to keep in mind as you tackle the security policy beast.

- **Develop policies that you plan to enforce**. A policy that you are unable or unwilling to enforce is useless. If your policy states that Internet usage is strictly limited to conduct business-related tasks, but you do not block site access or have the capability to monitor an employee's Internet activity, you should do away with the policy. A more reasonable approach might be to state in your policy that personal usage of the Internet should be restricted to breaks or lunch hours or to state that Internet usage is allowed as long as it does not interfere with employee productivity or meeting deadlines. Some Internet filtering and monitoring tools (discussed later) allow you to restrict or allow access based on time of day. For example, employees might be allowed to shop on the Internet over their lunch hour per your policy. If so, these sites could be made available during this time but restricted during all other hours.

- **Explain the purpose of the policy**. Policies should be developed with specific objectives in mind. Be sure to explain the need for the policy and specify what the policy is trying to accomplish. Some policy development guidelines suggest a format that includes a background section in addition to the actual policy statement. If you cannot explain why the policy exists, you cannot expect your employees to understand it or follow it. Get rid of it.

- **Develop security policies that do not require updates too frequently**. If your policies require frequent updates, they are probably too restrictive or too specific. For example, if you have a desktop operating system policy that states that "All desktops will be deployed with a Windows NT 4.0 operating system" you would have to update the policy as newer operating systems were released, like Windows 2000 and Windows XP, and the older ones become unavailable. In this example, a policy that states, "All desktops will be deployed with a secure, company-standard operating system" would allow more flexibility.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- **Differentiate between policies and standards or recommendations**. Your policies should be comprehensive and thorough but should not be so specific or detailed that what you really end up with is a set of best practices or recommendations instead of policies. Start with a high-level policy statement and then drill down to more exact specifications using standards and recommended ways to comply with the policy. For example, you could have a policy that states, "All data transmissions sent over an open network must be encrypted". Your company standard may specify that 128-bit encryption is required as a minimum encryption level. Your recommended encryption solution might be triple DES or AES. The key thing to remember is that as minimum encryption key lengths change or the encryption algorithm you prefer changes, your base policy would not have to change.

- **Don't develop your policies in a vacuum**. Since your security policies will apply to all employees across the company, it is a good idea to include employees from other departments in their development. Include at least one representative from each business unit in your policy development efforts. At a minimum, include a cross section of other employees in the policy review process. These individuals may think of something that you did not include and will provide feedback as to whether or not the policy is easy to understand.

- **Make your security policies available to everyone**. You can have the best policies ever written, but if your employees never see them or do not know where to find them, they will never be effective. Also, if they only see them at new hire orientation, do not expect them to remember and follow them. Policy distribution can be accomplished through many ways. Some software tools (discussed later) allow you to post policies on your company Intranet. You could always place a read-only copy of your policies out on your network in a publicly accessible directory. A complete hard copy of the policies can be distributed at employee orientation and re-distributed on a periodic basis.

- **Make sure your policies stay current**. While it is true that policies should be developed in a way that they should not be constantly updated, they cannot last forever without some modifications. If you do not have an existing policy on wireless communication and certainly on Internet usage, your policies are in desperate need of a refresh. Plan to review your policies on an annual basis and actually schedule the review. A good time to conduct this review could be at the end or the beginning of your fiscal year.

- **Make sure your policies are understood**. Develop policies that are straightforward and not too complicated. If employees cannot understand what the policy requires, they cannot be expected to follow them. A policy that is to long or complex will most likely never be read (in its entirety) and certainly will not be followed. Some software tools (discussed later) allow you to include simple quizzes with your policies to test an employee's understanding of the policy.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Review your security policies with new employees at orientation at encourage questions from them on anything that is not completely clear.

- **Require acknowledgement of your policies**. Always, always, always include an acknowledge statement with your policies and require that employees sign it. The acknowledgement statement should specify that the employee has received a copy of the policies, that they have read the policies, and that they agree to abide by the policies. Be sure that this signed acknowledgement form is retained in their employee file and that it can be retrieved if needed. Also, make sure that everyone in the organization has signed an acknowledgement form. No employee, regardless of their position, should be excluded from following the policies.

- **Include your policies as part of your security awareness training**. Plan to include at least one policy to be reviewed as part of your periodic security awareness training. This can be accomplished in many different ways. Reminders could be included as part of any classroom-style training. E-mail messages could be sent out on a regular basis. Banner messages that appear during login could contain a policy of the month reminder. The key is to raise awareness of your policies on a routine basis and use a combination of methods to keep a fresh approach that employees will notice.

- **Determine up front what is required to make a policy "official"**. Policies that apply to the entire company typically require approval from multiple levels within the organization. Make sure you know exactly what is required to make a policy active and who has to approve it. The amount of time it takes to get policies approved and deployed can be significant in some organizations. If you work in a remote site or are a smaller part of a large company, find out early on if global policies already exist or if they have to "come down from Corporate".

- **Make sure your legal department is involved**. Since your security policies are extremely important to protecting your organization and since failure to follow the policies could cause severe damage to the corporation and loss of employment to the employee, make sure that you obtain your legal department's review and approval of all policies. Failure to obtain this approval could result in creating legal issues for the company.

- **Stick to security topics for security policies**. Security policies only make up one part of an organization's total policies. If your assignment is to develop security policies, avoid trying to include policies that really should come form other areas. Examples include, human resource policies, procurement policies, or accounting policies.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Security Policy Assessment and Enforcement

After investing a considerable amount of time and effort in developing good security policies, you need to be able to determine if your employees understand them and are following them. This section includes tools and techniques that can be used to give you an indication of your policies' effectiveness or help you identify possible avenues for breaches in security. Some of these suggestions can also be used to help identify areas where additional security and policy awareness training is needed. In addition, some of the tools described below can be used to help enforce the policies that you develop.

VigilEnt Policy Center

VigilEnt Policy Center, from Pentasafe Security Technologies, Inc., is marketed as everything that you would need for security policies. This product addresses policy development, deployment, employee acknowledgement and understanding, and incident reporting.

For policy development, the Policy Center includes libraries of policies that can be used "as is" or edited to better fit your environment. The libraries include industry-specific sections (such as HIPAA for healthcare) that can save you time in your development efforts and also serve as a checklist to help you evaluate if a policy is needed for your organization. The licensing arrangement entitles you to periodic updates or policy refreshes for these libraries. Charles Cresson Wood, author of the book *Information Security Policies Made Easy*, developed the policies contained in the library.

For policy deployment, VigilEnt Policy Center allows you to publish your policies on your company Intranet and make them available to all of your employees. Employees can receive an e-mail notification whenever a new policy is released or updated that requires their review. In some environments, this may require that you have kiosk-type workstations in the departments where employees do not normally have access to the Intranet or e-mail from their desktops. After policy deployment, you can track who within the organization has accessed the policies and who has not. The product can also track user acknowledgement and acceptance of the policies, which can be very important in situations were policy violations are discovered.

To assist you with assessing the effectiveness of your policies, VigilEnt Policy Center includes quizzes that can be customized to test an employee's understanding of the policy. These quizzes are brief multiple choice or true/false tests designed to force the employee to read the policy and try to understand its meaning and not just check the acknowledgement box. This feature can also be used to help you determine if the policy is too confusing by monitoring if everyone misses the same questions. Management reports can be generated that indicate who has and has not read the policies as well as what individual or group of individuals may be having trouble understanding the policy.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A final feature of the VigilEnt Policy Center is the mechanism provided for reporting security incidents. Employees can go to the Intranet site and report any incident that they feel warrants investigation. The product also allows an employee to report an incident anonymously if they want their identities concealed. For this feature, it is critical that the issues reported are monitored and responded to appropriately.

PoliVec Builder, and PoliVec Scanner

PoliVec, Inc. offers a suite of products called PoliVec Builder and PoliVec Scanner designed to help you develop, assess, and enforce your security policies. This suite of products is targeted at network and operating system policies.

PoliVec Builder includes policy templates with best practice guidelines and additional templates that are more industry-specific (such as policies to comply with Gramm-Leach-Bliley). The policy templates provide text that explains the rationale behind including specific items as part of your security policy. The software also includes a warning mechanism to alert you if one of the best practice components is not included in your policy. The policies created using PoliVec Builder are designed for export and inclusion in PoliVec Scanner.

PoliVec Scanner is designed for use with Windows NT and Windows 2000. It allows centralized scanning and monitoring of multiple systems without requiring the installation of agents. The software scans to determine compliance with the set of policies developed using PoliVec Builder. The centralized control features allow administrators to make modifications to remote system settings such as password management, logging, and account lockout. For password management, weak passwords can be identified and either displayed or just flagged for corrective action. The product also reports on security-related registry settings, security patch status, and identifies system services that are present, but not needed. Management reports that summarize configuration results for each system can be generated following each audit.

Password Appraiser

Quakenbush Consulting, Inc. offers a product called Password Appraiser for Windows NT-based systems. This product is designed to provide capabilities above and beyond those already offered by existing NT password filters (passfilt.dll). In addition to enforcing password rules for length and composition, one of the enhanced features includes the ability to set password rules based on the type or level of user. For example, administrator password rules can be established that require that they be changed more frequently than those for “normal” users. In addition, the software can be configured to automatically respond to weak passwords that are detected. Options for the auto-response include disabling accounts with weak passwords, requiring a new password at the next logon, or sending an e-mail to the administrator.

Websense Internet Management Software

Policies that address Internet usage are a must for any organization. Even if you do not allow employee access to the Internet, you need a policy that states this. If you do

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

allow employees to access the Internet at work, Websense, Inc. has designed a product that assists you in managing Internet usage based on the policies that you develop.

Websense Internet Management Software interfaces with the appliance (firewall or proxy server) that governs employee access to the Internet. The product contains a large database of sites arranged by category that you can choose to block. The master database is updated on a daily basis. Management reports can be produced to monitor employee usage patterns and record the amount of time spent on the Internet. Websense also allows you to prevent unapproved file downloads that can create unwanted network traffic and introduce threats to your environment.

If your policy allows employees to access the Internet, Websense will support allowing access to specified sites based on the time of day. For example, if your policy supports it, employees can be allowed to shop on the Internet from the hours of noon to 2:00. The block on these sites is temporarily lifted during the hours you specify and then reinstated at the appropriate time.

E-mail Review

E-mail usage policies in today's environment are as essential as any that you have to develop. Appropriate uses of how the company-provided e-mail system is to be used must be defined. Periodic reviews of e-mail accounts can be very useful in determining if your policies are being followed. These reviews can also help identify possible espionage, and other breaches in security and confidentiality. At a minimum, for those who do not want to be viewed as "Big Brother", conducting reviews of e-mail accounts after an incident has been detected can provide very meaningful evidence when needed.

However, if you plan to ever conduct a review of employee e-mail, either manually or through monitoring software, there are some basic requirements that must be included in your e-mail policies. You must make it clear to employees that the e-mail system and all messages sent or received are considered to be company property. Explain within the policy or in user training the risks that can be introduced to the company through the inappropriate use of e-mail. Make sure to specify that employees should have no expectation of privacy for the content of their e-mail messages. State that the company reserves the right to monitor e-mail messages at any time. And always make sure that no single person is tasked with reviewing e-mail messages on their own. Involve at least two people authorized to carry out a review of employee e-mail and carefully document all aspects of the review and the results.

Internal Auditing

One of the best ways to determine if your policies are being followed does not require any type of software package. All you need to do is conduct an internal audit. A moonlight audit, so named because it is usually performed at night after your normal business hours, allows you to make one pass throughout your entire organization and assess numerous items related to compliance with security policies. This low-tech,

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

software free method of gauging policy effectiveness can be an eye-opening experience. An assessment of how many employees are following existing policies can be made as well as the collection of additional information that can be analyzed to help identify areas where new policies may be needed.

On the surface, conducting a moonlight audit seems pretty easy to do. However, in order for the audit to be a success, several critical factors must be considered. First, some things to keep in mind if you think an audit would be helpful in your organization.

- **Get approval to conduct the audit**. Make sure that you have approval from the proper authorities within your organization before you start roaming around your office in the dark. Also, make sure that your management has a clear understanding of exactly what the audit will try to accomplish. Finally, get the approval in writing and make sure that each member of the audit team has a copy with them during the actual audit. You may need to show this document to other employees working late, property management personnel, or security guards if you encounter any of these people while carrying out the audit.

- **Don't exclude anyone from being audited**. Every office and workspace should be included in the audit. Do not exclude your own department, your IT department, or your executive's offices. You might be surprised by how many high-ranking officers are guilty of security violations.

- **Keep the audit secret**. Involve as few other people as possible. Only disclose your plans to the people directly involved in supporting the audit. If you have to recruit help, ask for volunteers for a special after hours project and only give them the full details of what is to be done at the briefing before you begin.

- **Protect the audit team members**. Make sure that each audit team consists of at least two people. No individual should be allowed to enter your other employees' work areas alone. This measure provides more integrity to the audit and safeguards participants from being accused of removing personal property that may suddenly be reported as missing. Also, try to keep the names of the specific team members involved in your exercise confidential. Believe it or not, some people will not be pleased that you "invaded their privacy" by conducting your audit.

- **Randomly assign offices to be audited**. Everyone cannot go after the executive's offices. By the same token, team members should not be allowed to focus on only their friend's work areas.

- **Vary the days and times for your audits**. If you conduct multiple audits, and you should conduct these audits periodically, make sure that they are not all performed on the same day of the week or even at the same time. If the first audit occurs after hours on a weekday, conduct your next audit on the weekend and consider starting early in the morning. Just make sure that your employees are not able to

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

predict when you will strike or you may find that they put on their best security behavior only once a month when they think you are coming.

- **Use standard forms to record your findings**. Make sure each team uses the same approach to document what they identify as security infractions. A pre-printed checklist of the items to be audited works best and will reduce the amount of time it takes to gather the information during the audit. If possible, plan to enter all of the results into a database for further scrutiny and analysis.

- **Get an accurate floor plan**. Depending on the size of your organization, this is a must. Give each audit team a copy of the floor plan for the areas that they have been assigned. Each workspace can be checked off as it is completed to help ensure that all areas are covered.

- **Discuss possible scenarios the audit teams might encounter**. You might not be able to think of all possible scenarios that could be encountered, but spend some time thinking about them and prepare your team during the briefing. Some examples include what to do if the workspace to be audited is occupied by someone working late, what to do if PCs are discovered left on with files or e-mail still open, how to handle unsecured laptops that are discovered, but are not "standard" company equipment, etc.

- **Plan ahead on where confiscated items will be stored**. If you plan to collect items that are left unsecured, such as laptops, make sure that you have arranged for a secured area to store them until they can be claimed. One of the worst things that could happen is for the items you collect to walk out of the door before they can be returned to their rightful owners.

- **Involve your executives**. If possible, have the "victims" collect their unsecured belongings from an executive on the following day. Knowing that the president or CIO takes security seriously and is behind your audit will go a long way with the employees that are initially annoyed that their lack of security was discovered in your audit.

- **Make arrangements for the "early birds"**. If you confiscate laptops, you will undoubtedly have someone with a pressing deadline that comes in early the morning after the audit and finds their workstation missing. While it is true that a real thief could have taken their machine on the night before and never returned it, the intent of the audit should be to prove a point and not cause undue disruptions to your business or clients. Designate someone to handle equipment returns for these people.

- **Define very clear rules of engagement**. Make sure that all audit team members know the limits of how far to go to find security breaches. Rummaging through employees' office drawers for possible passwords while they are home sleeping

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

could be viewed as too invasive. However, checking for unlocked drawers that might contain a laptop when an empty docking station is discovered could be acceptable.

- **Document and share your results with management**. Prepare a complete report that describes all of the audit details and objectives, lists summary results, and specifies what actions will be taken for follow-up items. Be prepared to make the detailed audit results available on request. Save all of your documentation so you can make it available during an external audit if necessary.

- **Evaluate and rank your results based on risk**. Look at all of the information collected during the audit and decide what infractions introduce the most risk to the organization. Target remediation efforts for the more risky items first.

- **Use your results to provide awareness training**. Include results from the audit as topics for increased security awareness training.

- **Reward good behavior**. Consider acknowledging employees where no infractions were noted. Re-enforcing desirable behavior for those people that are following your policies is just as important as identifying those in need security reminders.

Once you have considered the suggestions listed above about how to conduct your audit, you need to decide exactly what you will look for. Many of the factors will show whether or not your security policies are being followed. The items listed below are some of the factors that can be included in your moonlight audit.

- **Is the office locked?** If the office being audited is equipped with a lock and the occupant locks the door on the way out each day, their workspace can be considered secure. If you can't get in to the space to look for other factors, you will have to move on to the next office. By contrast, office with locks that are not used should be noted.

- **Is the office occupied?** If the office occupant is still at work, you will have to skip the space and come back later, or audit the office at another time. If it is unusual for the employee to be working late, it should be noted. The employee's manager can determine if the employee was working late or potentially using company property for personal reasons.

- **Note the type of workstation**. Recording the type of workstation found in the office can be helpful to compare the findings to inventory records that show what was originally assigned to the employee. In addition, you may find equipment the employee has brought from home that does not meet company standards.

- **Is the workstation on or off?** If a PC is present in the office, note if it was turned off at the end of the day or if it was left on. If the machine is left on, determine if it

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

was secured (locked down) before the employee left for the day. It is not uncommon to find machines left on with files and e-mail left open.

- **Is the laptop unsecured?** If the office contains a laptop docking station, record whether or not the employee took the PC home or locked it in a drawer. PCs that are discovered unsecured can be confiscated. Leave a notice behind in the office that instructs the employee to claim the machine on the following day. Do not be fooled by just an empty docking station. Many employees remove the laptop from the docking station and put it in their desk, but they fail to lock the drawer.

- **Note personal property of value**. If you have a concern that employees bring valuable personal property into their office and leave it unsecured, make note of it for statistical analysis. Do not remove personal property as part of your audit. Examples of personal property to be noted include CD players, PDAs, expensive pen and pencil sets, etc. Companies cannot be responsible for the loss of personal property.

- **Note the presence of other office equipment**. Many times, employees may secure their laptops before leaving the office, but leave other expensive company property out in the open. Examples include proximas, hubs, routers, tools, etc.

- **Look for external modems**. External modems allow employees to bypass your company's firewall and provide a mechanism for intruders to gain access to your internal network.

- **Look for visible logon information**. Look for post-it notes left on the monitor that contain possible user IDs and passwords. Also, look beneath keyboards and mouse pads. It is not recommended that drawers be searched for this information.

- **Record the types and numbers of appliances**. Many office appliances such as space heaters, hot plates, and coffee makers can present a risk to the company if they are left on at the end of the day. Other appliances that draw more power can put a drain on your office electrical system and cause circuit breakers to be tripped.

- **Note the offices with no infractions**. Keep track of the offices where no violations are discovered. This information can be used to reward employees that seem to be following your policies.

Conclusion

Having a complete set of documented security policies should not be viewed as optional for any business. Keeping the policies that are documented updated is just as important. Only document the policies that you intend to enforce. Make sure that every employee has access to the policies, reads the policies, and acknowledges that they will abide by the policies. Include policy education as a part of ongoing security awareness training. Finally, identify and use mechanisms that help you determine if your policies

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

are complete, are understood, and are being followed. Like so many other things within the security discipline, developing good security policies requires careful thought and planning as well as ongoing care and feeding.

List of References

SANS Institute
SANS Information Security KickStart, (Online Training)
Intrusion Detection, The Big Picture – Part IV, Page 20

SANS Institute
SANS Security Essentials, (Online Training)
Intrusion Detection, The Big Picture – Part IV, Page 3

Pentasafe Security Technologies, Inc.
VigilEnt Policy Center
http://www.pentasafe.com
http://www.pentasafe.com/products/vspm.htm

PoliVec, Inc.
PoliVec Builder, PoliVec Scanner
http://www.polivec.com/
http://www.polivec.com/products.htm
http://www.polivec.com/polivecbuilder.html
http://www.polivec.com/pvbfeatures.html
http://www.polivec.com/polivecscanner.html
http://www.polivec.com/pvsfeatures.html

Quakenbush Consulting, Inc.
Password Appraiser
http://www.quakenbush.com

Websense, Inc.
Websense Internet Management Software
http://www.websense.com/
http://www.websense.com/products/about/howitworks/index.cfm
http://www.websense.com/products/why/index.cfm

Email-policy.com
Email policy: why your company needs one
http://www.email-policy.com/

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SANS Institute
The SANS Security Policy Project
http://www.sans.org/newlook/resources/policies/policies.htm

Risk Associates
http://www.securityauditor.net/
Information Security Policies & Computer Policy Directory
http://www.information-security-policies-and-standards.com/

Network & IT Security Policies
http://www.network-and-it-security-policies.com/
http://www.network-and-it-security-policies.com/policies.htm
http://www.network-and-it-security-policies.com/delivery.htm

Information Technology Management Institute
3-Day Network Security Course Including Moonlight Audits
http://www.itm-inst.com/itmi/Schedule/J3_02.doc

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.