Global Information Assurance Certification Paper

Title: Security Policies: Where to Begin
Name: Laura Wills
Date: December 12, 2002

Introduction

A company that realizes that they have unfortunately been applying security in an ad-hoc fashion and have not put the necessary security policies in place to reduce the risk to their corporate assets, has hired you as the Security Officer. They have implemented many of the standard security products and technologies (firewalls, anti-virus, IDS, etc.), but without the policies and processes defined, they find viruses and intrusions still occur. As the newly appointed Security Officer you are to develop their security policies and procedures from top to bottom to provide a cohesive approach to addressing security going forward. This is an enormous job; where do you begin?

Many organizations and their staff truly lack the understanding of what security policies are designed to do. Your mission, should you chose to accept it, (it will feel, at times, like "Mission Impossible") is to educate all levels of the organization on how they play a role in identifying potential threats; when to escalate, and to whom, so the risk can be assessed and a mitigation strategy developed.

The intent of this paper is to guide you through the process and considerations when developing security policies within an organization; however it will not attempt to write the initial policies. There are a multitude of excellent websites and software products available that can assist with the actual development and provide sample formats.

Understand the Business

In order to develop a realistic security policy you have to understand the business and how they generate revenue. This will determine which policies will have a higher importance to the executives and the shareholders. If the executives are aware of the threats, risks and potential exposure to the company, they will ensure funding is allocated to deal with the issues you may uncover during the security policy development phase.

Every company wants visibility on the World Wide Web, but at what cost? If they are not willing to make available the necessary funds to implement a sound secure infrastructure or the time to develop the personnel skills to maintain it, then maybe they should consider hosting the website with an external reputable firm. If they decide to go this route, then ensure the same security policy principles are applied. Interview the potential firms on their security policies and practices. Moving the managed service does not necessarily mean you have removed the threat.

Understand the Security Officer's Role

As the Security Officer, you bring experience, process, best practices and guidance to the organization. It's your job to inform, advise and receive acceptance on the security policies. Once a policy as been agreed to, it will need to be reviewed and approved by the authorizing individual or committee. Don't be surprised if it is sent back for revision. The best policies are developed over time. Consider every policy as a living document that will need to be revised as the environment, business direction and technologies change.

Know Thy Players

You've got to start where it makes sense. You need to determine who will be involved in the development and authorization of the policies. If you don't know who will authorize the policies, how are you ever going to complete the task? It is essential that you understand the reporting structure and company culture. This insight will help you understand the political environment that lives within every organization and who the influencers and decision makers are. The CIO and IT manager are going to become your new best friends. Walk a mile in their shoes to understand the organization; why things are the way they are; as well, what the business and technology vision is. This is not to say that just because that's the way it was done in the past, this is how it should be handled in the future. There may have been barriers in the past that prevented them for doing the job right in the first place.

Interview the key hands-on resources that are responsible for managing the existing infrastructure. This should include network and database administrators, developers, architects, PC and help desk support. What's their mandate? Do they have a mandate? Or is their workday typically a response by reaction. How do they verify staff for password resets, and system or file access? Request any documented processes and procedures. Even if it hasn't been documented, do they informally agree amongst themselves on processes? Example: Password length and character mix, renewal criteria, failed login attempts, etc. Now is the time to uncover any informal security practices. If there are written policies, find out if they have been signed off by an authorized individual, who that person was and if they are still within the organization?

Get to know the company's Legal, Audit and Human Resources personnel. Legal will need to be directly involved in the wording and implications of policies that are external facing, such as login banners, connectivity and information sharing with third parties. HR and legal will need to provide guidance and input for policy violation clauses and their enforcement. Audit will advise on what they look for when conducting a network security assessment.

Forming the Security Policy Committee

The purpose of the Security Policy Committee is to ensure the policies meet the needs of the organization. Buy-in or adoption by the organization as a whole will happen much quicker if policies are developed as a group, than if you present a

policy and instruct staff to adhere to it. The committee is made up of people who will provide the reality check. They will be the ones that know, after a great deal of discussion, whether a policy can realistically be enforced and managed.

As the facilitator of the security committee meetings, it's your job to get the right people together and mediate to get consensus among the team. It is advisable to include representatives from different business units and various departments. The business units typically understand better than anyone, what the value of the data is, what needs to be protected and to what degree. Also, you will need to understand what the potential threats are if you decide to abstain and do nothing. Different people will have different perspective on what needs to be protected. Respect and evaluate those differences. Be prepared to manage and facilitate those differences before they become heated arguments. Conflict can become a barrier to understanding or listening. Ensure there is an IT representative on the committee, as they typically have to change the most to enable a policy (technologies, architecture, processes and procedures).

The team will be looking to you to initiate discussion and expedite the process. As you uncover formal or informal policies you want to ascertain what the policy was trying to achieve and if it needs to be refined? Present options as a starting point and adapt to the needs of the organization. Two questions that need to be answered for every policy are: What are you trying to protect? What are the potential threats? It is advisable to sometimes only include a sub-set of the committee for policies that only relate to certain groups; otherwise you run the risk of committee members not attending when their input is really required.

Legal, HR, Audit and the authorizing body need to be a part of the committee, but may or may not attend the meetings on a regular basis. That's okay; they're busy people, as long as they are kept in the loop to provide timely input and feedback.

Security Policy Development Approach

Begin the policy development like you would any project. Understand the requirements, where you are today, the desired end-state and how you're going to get there.

Security policies are the enablers for IT professionals to do their job effectively; pro-actively rather than reactively. A policy statement that states a network vulnerability scan or penetration test will be done on newly developed systems prior to implementing into production environments, has effectively given IT permission to conduct this activity in a timely manner, without having to request approval each and every time.

You need to consider the present level of risk to the organization, Conduct a risk analysis, and then prioritize which policies to begin with first. For example, if your websites are consistently under attack then the company's credibility is at stake, even if the information on the site does not pose a financial or liability risk, it does

pose a threat to the company's credibility. It doesn't take long before the black hat community spreads the word that you're an easy target. Depending on the present level of risk, it may be best to start will the simplest policy and work your way through to the more complex and challenging ones. Complex policies can get caught up in the review process for a lengthy period and you could lose your momentum. It makes sense to run a few policy developments simultaneously; the high risk and simplest in parallel, but don't over-whelm the security development process.

Once the committee or sub-committee members agree on the finished product for each security policy, it's time for the signing authority to become actively involved. It is important to communicate and agree on the expected turn around time. If you fail to set expectations then the review process could drag on indefinitely. Don't stop and wait for the approval of one security policy before starting work on the next one, in order of priority.

Defining Security Policies

As defined by SANS, policies describe "purpose, scope, policy statement, standards, action and responsibility". Where possible, policies should be written to minimize the effort to maintaining them, yet be clear in the objective, boundaries and procedures to enforce them. Consider when an "exception to the rule" clause needs to be included so there is flexibility when circumstances demand it, but those exceptions should be clearly defined.

Program policies are broader in scope and generally apply industry standards, such as ISO 17799. Issue-specific and System-specific policies are designed to meet the organization's unique requirements.

You can anticipate that system-specific policies will be written with a particular technology and product in mind (i.e. Windows 2000, Linux, Solaris, Cisco Pix, Check Point, etc). Expect these types of policies to be revisited more frequently as the technology revolution continues. The "purpose, scope and statement" should not need to be changed, but the "standards" and "action" might.

The next section will look at some of the considerations for the more commonly developed "Issue-specific" and "System-specific" policies that reside within an organization. Different companies have different security policy needs; the actual number and type of policies to be developed will depend on your company's needs.

Passwords

The simplest security policy to review and build upon is the password policy. Understand your user community and habits. Are they mostly administrative, business or sales people? Are many of them away from the office frequently and do not have easy access to IT staff? If you impose mind-bending passwords, they will likely forget their password and store them inappropriately (i.e. paper,

unencrypted files, PDAs etc). Look at using best practices, but adapt to what is realistic for your environment.

Logon Banner & Email Disclaimer

Develop a policy to ensure all login entry points have a banner page that notifies the users that only authorized individuals are permitted to use the system. As well, a standard e-mail disclaimer should be implemented for e-mails distant for external parties. Get the legal department involved in the wording.

Laptop Usage

Review the PC usage policy and distribution method. Does the company mostly use laptops that if left unattended could be picked up and walked off with? Does the company provide laptop locks? Laptops have been known to walk out the door even during business hours. Does the company have a clean desk policy? During after-hours and weekends are laptops locked in a secure drawer? Is the key left in the drawer? Can the drawer be opened with a simple tool, such as a screwdriver or letter opener? Don't under estimate your perpetrator. I once heard of an individual that had gained access to a secure building, through the company's card-access doors and was under the desk prying open the draw when the security guard came upon him during a routine floor check. It was later discovered that the individual had used a screwdriver to open the locked stairwell door located by the receptionist area. He easily gained access to other floors by using the visitor's pass that was in the receptionist desk. He was able to move from floor to floor without being detected, as least not suspiciously. The company changed their policy so that visitor cards where deactivated at 5:00 p.m. each business day and metal plates were installed on the stairwell doors. Implementing these policies minimized another risk in their security infrastructure.

Once the laptop and data that resides on them leaves the office what means does the company have to protect the assets? What is the risk and liability to the firm if it were to be stolen? Does the corporate information residing on the laptop, which if fallen into the wrong hands and made publicly available, jeopardize the company's position or reputation? Is the laptop used to connect back to the corporate network? By what means is this permitted (i.e. remote VPN, PC Anywhere, dial-up accounts)? Is the laptop used at home for personal use (i.e. games, non-corporate software)? What is the policy for non-corporate sponsored software on company owned computers? These are some of the questions that should be asked to develop a sound policy. Statistics show that computers, among other electronics, are the most likely thing to be taken from a home. The smaller the electronics the more likely it would be taken in a grab and dash scenario.

Anti-Virus

Once you've finished reviewing the password and physical aspect of computing, let's look at the anti-virus program. I would like to believe most organization have implemented an anti-virus program for their end-user's PCs. The user should not have the capability to disable the software or decline the distribution. Take a look at what's in place. Who's anti-virus software does the company use? Are they a well-known vendor and provide frequent updates with ease? How quickly after a virus becomes known does the vendor provide a new signature? Has the IT department had any issues with technical support in the past? How are updates distributed to the end-user? If you have a software distribution product, use this method to update the PC during the next reboot. Always, and I do means always; test the update and distribution method in a controlled lab environment first. Can you imagine the embarrassment of distributing a virus through the very means that you are trying to protect the company? Or if the distributed program was not well tested and renders the PC non-functional? Trust me, the executives will be asking a lot a questions and your reputation will be at stake (That kind of visibility on the masses will not help your career!).

Take the Anti-virus policy up to the next layer. Many viruses come by means of e-mail. Have users been educated on e-mail ethics? Things like, never detach a file from an unknown source. Do not (re-iterate this), forward on e-mails that tell you to do exactly that, to all your co-workers, friends and family. Leave the notification job to the professionals; contact your IT department. After a few frantic phone calls from end-users, the IT staff will likely send out an all staff e-mail advising staff how to behave. Consider how the Anti-virus policy should be included in the user education program.

If you know that e-mail is one means by which viruses are delivered, look at what programs are in place to stop it before it reaches the end-user. Anti-virus on the e-mail and other servers is a smart choice. Gateway ant-virus might be the right decision (ftp, HTTP UDP scanning). But consider the trade-offs; latency due to the e-mail scanning process verses the risk to the company, etc.

Network Systems

Based on well developed policies, IT staff should be able to define the procedures to ensure they are kept up-to-date on patches and fixes as they become available. Again, before updates are applied in a production environment, do this in a controlled, simulated (if possible) test environment first. IT staff should subscribe to vendor and security news groups to stay on top of new vulnerabilities, patches and fixes as they become available. Understand the relevance of the patches or fix to the environment you are trying to protect. If a new patch or fix is related to a service you don't use, consider whether it should be applied. But also note, even if you don't use the service today, you may in the future and will you remember to apply the patch or fix then?

Review the authorization levels required to manage the systems. Minimize the use and knowledge of administrator or root logins and passwords. Even system administrators should use a personal user ID with minimal privileges as their default login. They should only use the more powerful ID when a situation calls for it. I speak from experience, when I tell you that 9 years ago I infected an entire network because the financial executive asked me to look at a problem he was having on his PC. I logged onto his PC using my god like privileges. I soon discovered he had a virus on the PC. He had installed a rental game for his son's enjoyment on a corporate asset. When I logged in I infected the login.exe file. As staff returned from lunch, voila the majority of PCs on the network were infected. I had to immediately shutdown the network to contain the spread of the virus. It took a swat team a full day to clean up the problem. Several security policies would have mitigated this risk (i.e. software usage, anti-virus, login privileges).

A full audit of directory and file permissions should be conducted on a regular basis. The policy should outline the process; who is responsible to carry out this activity and the frequency it should be performed.

Controls should be in place to limit the number of personnel that have physical access to the systems. If the systems reside in the computer room, review the access list and activity log. Are the logs reviewed daily, weekly or monthly and by whom? Do the cleaning staff have access to the room? Does the employer provide a police check on the staff and are they bonded?

System Backups

Back-ups are a key component to any network infrastructure. It may make sense to implement High Availability (HA) for critical components of your network. Look at the single-points-of-failure and what the risk and liability would be to the firm if they were unable to operate in a normal fashion. What's the impact to the business if the Internet link should go down? Are you delivering services to clients through a website or portal? Are there financial consequences if you are unable to meet a SLA or take orders? If HA isn't a necessity, than what's the maximum outage that can be tolerated before it impacts productivity and/or business? What are the processes to recover a network, system, file, etc? Who is responsible for determining the business continuity program? To what degree should the plan consider; a system failure, a building power outage (short-term verses long-term), a full disaster, such as 9/11? Once again, a security policy is designed to protect the corporate data and has to take into consideration the data recover process for any mishap and event. The backup strategy should be reviewed in detail. What is the backup process? Who is responsible? Where is the back up media stored and when should it be sent offsite? When does it return? What are the legal requirements for the data retention? How frequently does the IT department test the recovery process and what is the procedure? Is a hot-site or warm-site required to address the companies business continuity strategy?

You will likely require upper management and legal representation to answer many of these questions. Don't wait until the committee has developed a policy before getting the required input. Don't forget to look at your back up strategy for router/switches configuration files as well.

Network Connectivity

Take a look at how IP addresses are assigned to servers, printers, PCs. What factors determine when DHCP or static IP addresses will be assigned?

Are un-used data jacks in publicly accessible or common areas active in the wiring closet or switch port? Are you using wireless Multi Access Points (MAP)? How are the devices authenticated? Without deactivating un-used data ports or a wireless security strategy in place the company is at risk of unauthorized access to the corporate network and its data.

Is the company's DNS a tattletale sign of the network layout? Where does it reside; private or DMZ network segment? Imagine the impact to the company if the DNS server is compromised.

Is the wiring closet locked or is it publicly accessible? If anyone can access the hub or switch, then they can plug-in and get access to the company's data. Many Cisco switches come with a serial port; this is another means by which a malicious perpetrator can compromise your network. Remember many switches/routers are often managed remotely. Password length and renewal practices need to be enforced. When it comes to administrative passwords on servers and switches/routers; minimize the number of people that need to know this information, but make sure it's greater than one. The security policy will assist in the development of procedures to manage many of these network infrastructure protocols and devices.

Network Security Architecture

If the company has an existing firewall, review the change management process. Who are the administrators? Do they have a formal review process prior to implementing a change? Who approves the change request? Technical personnel are not necessarily the right people to determine if the firewall change should be done. You should have the data owners approve the change request. This approach moves the decision and liability from technical staff to the business units. If a security architecture matrix doesn't already exist, then one should be developed. The matrix helps guide the firewall administrator on what network segment permit traffic inbound and/or outbound. A proper firewall design and matrix should almost never allow inbound traffic to the corporate or private segment from a publicly accessible segment, such as the Internet and DMZ. It's common for large organization to have multiple DMZs to accommodate different security needs or trusted partner relationships that share information. Consider putting database servers that support a public website in a different DMZ than

where the public web server resides. This approach is a best practice as it secures the database to known traffic, as well provides an audit trail.

Remote Access
Review the network access permitted by third parties, either as a client or business partner. Do they come in through the firewall or by other means? Whatever the method is, a policy needs to be in place ensuring that there is an audit trail and the access rights and logs are reviewed regularly. As the Security Officer you need to be aware of the business arrangements with third parties. What has been promised from a contractual point of view? If the arrangement is to provide access through other means that bypass the firewall, look at the authentication method. What auditing methods are in place to ensure they are who they say they are. Does the company use CAs (Certificate Authority)? Is the company using a remote client VPN solution? What are the reasons for not going through the firewall?

Review what the liability or penalties are should a security breach occur to either party by means of the other party's network. Ask the question, what the consequences are if confidential information falls into the wrong hands, such as financial or software code. Hopefully the lawyers have dealt with this issue and written it into the contract. Review the contracts to ensure the infrastructure supports the contractual obligations. Remember a company's image and reputation is important and has a value.

Other Considerations

Vendors Selection
Consider the vendors that you chose to do business with. Do they turn around new patches in a relatively short time after a new vulnerability has been identified? Know the financial stability of the software and hardware vendors you do business with. If their financial stability is in question, you could find yourself in a pickle if the company goes under or changes ownership. Nothing can be worse than when a company has made a substantial capital investment on a software or hardware product and the company ceases to exist.

Security Training
What is the security awareness and skill level of the individuals that are charged with managing the environment? Network Security is dynamic; the company must be committed to training and re-training resources to enable them to act appropriately to secure the infrastructure. They need to know what procedures and protocol to follow when a real threat occurs.

You may be asked to qualify the cost for training staff on security related products and topics. If the costs are too high the company may want to reconsider outsourcing a certain component of the corporate security (i.e. firewalls, IDS, routing & web hosting). If the company is only prepared to train

one individual and that individual does not provide knowledge transfers to others or leaves the firm, you're right back to where you started. Don't forget training for the Security Officer is just as important as it is for the technical guru's that will act on the policies. Security seminars and symposiums are valuable to staff because they can learn a great deal by networking with their peers and keep on top of the latest security threats and available products. Certification is nice to have, but depending on your business, may not be a requirement to demonstrate staff capabilities. There are plenty of good people out there that do not have certification. On the other hand certification does say that the individual is trained and comprehends the subject matter. Find out what the company's views are on this subject.

Security Violations

As the Security Officer you should understand how the company wants to proceed when a security policy violation has been uncovered. There will be different approaches to consider depending on the severity of the violation. A password violation may only consist of an e-mail to the individual and maybe CC the individual's boss. If there is continuous offences of the policy by the same individual, stiffer actions may be required (i.e. a letter on the employee's file to be included during their next performance review). Severe security violations (i.e. proprietary and confidential company information leaving the firm), may suggest that an individual be terminated immediately. These types of security policy breaches should be communicated, with clarity, to all staff. Legal and HR involvement will be required. Depending on the sensitivity of the business, you may need to recommend software that will search the content of e-mails for certain keywords. Again, staff will need to be advised if this is occurring or potentially could take place.

Policy Awareness Program

The awareness program you develop will educate staff on what is an asset and what should be considered a threat. A threat can be classified as anything that attacks the Integrity, Availability and Confidentiality of corporate assets. Once a security policy has been signed off, make any necessary infrastructure changes and develop the procedures to enact the policy, before communicating the policy to company staff.

Determine the best means to disseminate the policy information to staff. Policy information could be distributed to employees using the company's Intranet website and/or handbooks that are given out during orientation. The only problem with distributing security policy by way of a company Intranet is you run the risk that the end-user will not have read it.

PJ Varrassi gave the following advice during a "security policies in the workplace" webcast.

> "Have workers READ and SIGN an agreement that states they will abide by policies, procedures and technical controls implemented."

Another approach to advising staff of a new policy is to include it in a monthly newsletter that could be electronically sent out to all staff. You could design the e-mail with an acknowledgement mechanism in mind. Many e-mail products have the means to do this. New hires should sign the agreement during orientation and before a user ID is assigned.

You may want to consider grouping many security policies together for a monthly or quarterly publication. Lunch and learn sessions are a great way to inform and demonstrate the importance of security to the organization.

If HR conducts "new hire" orientation sessions, ask if you can take 30 minutes to provide a high level presentation on the company's security policies. The presentation should cover the importance of security to the company; how polices are enforced; the role each employee plays in maintaining security; what action will be taken for violation; where to find the information; how they can expect to receive updates; and who to contact with questions regarding policies.

Security Policy Effectiveness

What good is a policy if you don't take the time to measure its effectiveness? A yearly policy review process should consider how effectively the policies align with the business objectives. Security policies are not a write once and forget; they are living documents that will need to be reviewed periodically. The frequency will depend upon the nature of the policy.

Revisit the risk analysis that was conducted at the beginning of the policy development phase, then measure how well the policy has prevented, corrected and detected the threats to mitigate the risk to the company's data.

Conclusion

Your job as a Security Officer is to bring experience, process and guidance to the table, not dictatorship. Effective security policies cannot be written in isolation. You are the facilitator, bringing the right resources together to provide input and guidance in the development process. If you don't get buy-in, staff will find ways to circumvent the security measures you put in place.

Policies are written to enable professionals in the organization to act. A policy should not be written in such a way that it disables staff from doing the right thing when unique situations occur. There are going to be exceptions to the rule.

Ensure that staff are empowered, trained, and prepared, without abusing the authority, to enforce security policies; otherwise they will not be taken seriously.

The Company executives and business leaders must be committed to the security policy process and promote adherence.

Security policies are living documents and must be reviewed as circumstances change.

Policies have to be written with clarity and readability to the lowest dominator. They must be readily available and easily accessible to all staff. Work with the Legal, HR, Audit and IT departments to make this so.

References:

Hurley, Edward. "Company Tackles Wireless Network Security Risks." November 15 2002
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci863699,00.html

Varrassi, PJ. "Security Policies in the Workplace." Searchsecurity.com. March 29, 2001
http://searchsecurity.techtarget.com/webcastsTranscript/0,289691,sid14_gci531240,00.html

Guel, Michele D. "The SANS Security Policy Project." SANS Institute Resources.
http://www.sans.org/newlook/resources/policies/policies.htm

Andress, Mandy. "Effective Security Starts with Policies." Nov. 16, 2001
http://www.infoworld.com/articles/tc/xml/01/11/19/011119tcpolicy.xml

Pereira, Brian. "Security Policies: The Right Approach." Network Magazine.
http://www.networkmagazineindia.com/200211/cover2.shtml (Nov. 2002)

Pereira, Brian. "How Effective is your Security Policy." Network Magazine
http://www.networkmagazineindia.com/200211/cover1.shtml (Nov. 2002)

Control Data Systems Inc. "Why Security Policies Fail." Copyright 1999
http://downloads.securityfocus.com/library/Why_Security_Policies_Fail.pdf

Information Security Policy & Standards Group. "The Information Security Policies / Computer Security Policies Directory." Copyright 1993-2002
http://www.information-security-policies-and-standards.com/

Barman, Scott. "Writing Information Security Policies." November 9, 2001
http://safari.informit.com/?xmlid=1-57870-264-X/ch02#ch02

Avolio, Frederick M. "Best Practices in Network Security." March 20, 2000
http://www.networkcomputing.com/1105/1105f2.html?ls=NCJS_1105bt

Policy Development References:

Cresson Wood, Charles. "Information Security Policies Made Easy". Baseline Software. 1996
http://www.pentasafe.com/news/viewpr.asp?ID=105

Cresson Wood, Charles. "Information Security Roles & Responsibilities Made Easy". Pentasafe Security Technologies
http://www.pentasafe.com/publications/pdfs/R&R_4pp.pdf

COBIT
http://www.isaca.org/cobit.htm

VigilEnt Security Management Solutions
http://www.pentasafe.com/