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

R. Wayne Kirby
Version 1.4b

Title: Security Policy and the New Information Technology (IT) Manager

Introduction: The Information Technology (IT) Manager has just resigned and you have been promoted to this position, what next? Or, you were just hired by a start-up company as an IT specialist and found out that you are the new security expert, where do you start? This document delves into these possible scenarios and some suggested guidelines for an IT specialist new to the Information Assurance (IA) or Network Security Field. The first scenario looks at reviewing what a hypothetical Security Policy might contain and why, while the second scenario investigates steps involved in creating a Security Policy for your company. The majority of the guideline information was gleaned from various web sites, which will be mentioned in the text and again in the Resources and Additional Information section.

**Scenario 1:**
You are employed as a senior-level IT Specialist for a mid-sized law firm located in a large metropolitan area. You have been with this firm for four years performing network administrative duties and supporting the corporate Help Desk. During the past year, you have heard rumors about disagreements between the IT Manager and the corporate management. Early this morning, you were summoned to the Senior Partners office and informed that the IT Manager quit without notice earlier in the morning and you were being promoted to IT Manager effective immediately. The Senior Partner has Domain Administrative privileges and has provided your user account with Administrative access. Your first assignment is to remove all access the former IT Manager had and ensure he has no way to access the firm's information system. Additionally the partners have decided that they wish to ensure the safety and security of the corporate data and want you to provide them with a brief on the security policies and procedures the IT department has in effect to protect this data and the corporate IT communications system. Where do you start? When faced with challenges of this type, it is probably a good idea to first disable the user account of the former IT Manager and ensure no back-door access has been put in place. The SysAdmin, Audit, Network, Security (SANS) web site offers a good primer on Security Policies from Michele Guel's course "Proven Practices for Managing the Security Function". The primer is available at http://www.sans.org/resources/policies/#primer and can provide guidance in reviewing your company's own policy.
To meet the management requirements, a good place to start is with the Corporate Security Policy and the following questions:

Does the corporate policy establish IT departmental security responsibilities?
Does the corporate policy include a security policy for IT systems and information?
If an IT policy does exist, does it meet the requirements for confidentiality, integrity, and availability? If no policy for the security of IT systems and information exists, what is required to implement one? (Refer to Scenario 2)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

If an IT policy does exist, the next step is to review this policy for conformance to the three security principles of confidentiality, integrity, and availability. The COAST, Computer Operations, Audit, and Security Technology web site, now known as CERIAS provides basic information on Security Policy and more in-depth information on items a security policy should contain, such as intrusion detection (http://www.cerias.purdue.edu/coast/intrusion-detection/policy.html).

To meet the confidentiality, integrity, and availability principles requires a Defense in Depth strategy comprised of multiple levels of physical and application security, personnel training, and a maintenance and management policy for each. A review of the existing policy should include the following:

Does an Administrative Management policy exist for your network? This includes the management of user and computer accounts and the group memberships and permissions assigned to them. This policy should establish who is authorized to create user and machine accounts in the domain and who can authorize the different levels of permission or access users can have to the different hardware and information on the corporate network. For example, the Human Resources manager should not be authorizing access to client data files for pending cases and the Paralegal Department manager should not be authorizing access to payroll and human resources data files. The IT Security Policy should refer to the Administrative Management Policy to determine the respective departmental manager or work center supervisor with authority to authorize employee access.

Does your network include one or more type of perimeter defense consisting of intrusion prevention and detection systems such as firewalls and Intrusion Detection Systems (IDS)? Does your security policy include maintenance and management policies and documentation standards for these systems and are they enforced? Simply having a firewall setup between your network and the outside world does not ensure protection. Proper configuration of the firewall and periodic review of the configuration will help to ensure the best possible protection. The configuration should be documented according to an established Configuration Management Guideline and the documentation updated to reflect all changes to the firewall configuration. Of course this documentation should be maintained in a secure location with access limited to appropriate personnel.

Does your security policy include intrusion testing and define how, when, and where the testing will be performed? Believing that your firewall is properly configured does not prove that it is actually protecting the assets you have decided to protect. Intrusion testing is a matter that requires very careful planning. Remember, your testing could result in actual failure of your network. Intrusion testing should be seriously reviewed with management and have the complete approval of all management. You may be the IT Manager but the Corporation owns the network, you should never undertake this type of testing without the complete approval and permission of the network owner.

Does your network include hardware and software protection through the use of system auditing and IDS to provide protection from accidental and malicious attack from internal and external sources? Internal attacks whether intentional or accidental are a major source of concern. According to the 2002 CSI/FBI Computer Crime and Security Survey, available at http://www.gocsi.com/forms/fbi/pdf.html, insiders

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

committed 38 percent of unauthorized access and 78 percent of abuse of network access. Most network operating systems include built-in auditing software. Proper auditing will identify the office receptionist who has been accidentally given inappropriate permissions to data files as well as identify malicious attacks. A thorough review of the documentation for the network operating system in use may provide correct auditing configuration information. If this is not the case, then, third party documentation or training should be considered. Most commercial IDS systems are designed to audit port and protocol access attempts and will provide more in-depth information of the attempted access. When properly configured and monitored, some IDS can provide notification of particular types of attacks while the attack is in progress as well as the source and destination Internet Protocol (IP) addresses. This information can be a tremendous help in firewall configuration so regular review of logs should be included in any security policy. Remember, having information available does nothing to help protect your assets. Review of the information is what leads to changes in security posture.

Does the IDS deployment in your network really meet the determined corporate security requirements and does a management policy exist for any deployed IDS? Does your network have an Internet presence? If so, what procedures are in place to protect outward facing assets from malicious attack? If an ISP provides your Internet presence, what methods is he employing to protect your asset? Does the ISP policy meet or exceed the corporate policy requirements?

If you maintain your own corporate domain and Internet presence, what protections are in place to prevent intrusion into your Domain Name Server (DNS)? If an attacker can compromise your DNS, he can wreck havoc not only on your corporate network but also to other networks and the Internet itself in your name by using your network as an email forwarder. Proper configuration of DNS is of utmost importance. Improper DNS configuration or routing can cause loss of name resolution resulting in a communications failure on your network. Any changes to DNS or routing within your network should be reviewed by a team of personnel knowledgeable and experienced in network management prior to configuration changes. The Configuration Management Guideline should include a section covering DNS and routing configuration.

Another type of attack on networks is through virus and Trojan software. Does your network include the use of antivirus software to protect workstations and servers from malicious attack from the Internet and email? Does a management policy exist and is it enforced? According to the 2002 CSI/FBI Computer Crime and Security Survey, viruses caused 85 percent of network attacks or misuse. Many employees work at home as well as in the office and must carry the data back and forth. Not knowing the security profile of each individual employee's home computer is a nightmare for any IA person. Employees may innocently introduce a virus or Trojan into your network in this manner if virus protection is not deployed. Ensure the antivirus software is deployed to all workstations and servers and that the software is configured via administrative console to provide the best possible protection for your network environment. Ensuring scan engines and virus signature files are kept up to date will provide the best protection offered by the product. Removing configuration access from the local user will prevent any accidental change to a workstation or

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

server that might result in the introduction of a virus or Trojan into your network. Having an antivirus application is one thing, having the application actively protecting the computer systems is another; no employee using corporate network computers should have the ability to disable software.

All configured audits whether preformed by the operating system or other software/hardware combinations should be saved to logs, as these audit logs may be required to assist in personnel or legal actions. These logs can also be used to show what protection and detection methods were in place if your network is successfully attacked which can help determine where the attack occurred and where it originated.

What is the corporate policy on using or installing personal software? Allowing network users to install their personally owned software can lead to possible licensure issues as well as problems caused by Trojan or virus infected freeware/shareware. Providing unsuspecting individuals with freeware is a major method of spreading Trojans and installing backdoors in well-protected networks. The most highly recommended procedure is to allow only authorized IT personnel to install software on workstations and servers and to allow only software purchased and licensed by the corporation to be installed. Consideration should be given to an enterprise inventory application to monitor and maintain hardware and software inventory of the network. Some of these applications include software license monitoring and can alert you to the installation of software not licensed to the corporation. All software should of course be tested in a test environment prior to being installed or distributed on the network. If corporate policy does allow the use of personally owned software, this software should be examined for viruses and Trojans by IT personnel before installation on any system in the corporate network and installation should still be limited to authorized IT personnel or a network system management application.

Is the security configuration of the network operating system in use, both server and workstation versions properly configured to provide the highest possible security profile while still being productively useable? Many web sites exist which provide security configurations for different versions of the Unix or Linux kernel as well as numerous publications and books. Microsoft provides security configuration and best practices guides for its current and still supported operating systems on its TechNet web site http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/howto/sechow.asp. Care should be exercised when implementing operating system security lock down to ensure the operating system is still useable after security configuration.

Does your policy include procedures for incident handling and recovery? The article, Incident Handling by Rik Farrow viewable at http://www.networkmagazine.com/article/NMG20000515S0109, provides some basic recommendations of steps to take when it is determined that an incident has occurred. Documentation is of utmost importance when investigating a suspected incident. Documentation makes possible peer review to determine the nature of the incident and possibly to help identify the party or parties responsible. Remember, the idea behind networking is distribution of information and applications, the bad guy

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

knows this well as represented by some recent distributed denial of service attacks so identifying a perpetrator is not an easy thing.
To quote Rosemary Sumajit in her paper, Developing Security Policies: Charting An Obstacle Course (http://www.sans.org/rr/policy/course.php), “Even though we may use the word security, we are really talking about taking measures that will reduce the likelihood of danger or mitigate the effects of a breach. We are actually talking about managing risk”. Since any network could possibly be breached, it is also necessary to have steps in place to recover from an incident. These steps include a backup policy to ensure critical systems are backed up on a regular basis and the backups are tested. It doesn’t help you to find out while attempting to return the network to operation after an attack that the most recent backups of the domain controllers or global catalog servers are corrupted.
Finally, does your policy include an acceptable network use policy and training for network users to ensure they are aware of use policy and the various security threats discussed in previous paragraphs? All users should be required to read and acknowledge the acceptable network use policy as well as view a short presentation on network security threats. The policy should include refresher requirements for the training of network users.
A security review performed in this manner should provide a good overview of the corporate security posture for presentation to management.

**Scenario 2:**
As an Information Specialist with fourteen years of experience you are looking to broaden your horizons and improve your checking account balance so you apply for a Network Management Specialist position with a new start up business in your town. Your resume indicates that you have experience installing and configuring both Intrusion Detection Systems and firewall applications. Two weeks later, you start to work. After the niceties of HR check in, you report to your division manager for your job assignment. This is when you find out that you are the Team Lead for the Information Technology security team and are to develop a security policy for the corporate IT assets. Installing and configuring hardware and software doesn’t seem to fit in with policy development so, where do you start?

**Beginning**

The terms ‘should’ and ‘will’ are used throughout the following discussion. The term ‘will’ indicates a requirement and the term ‘should’ indicates a recommendation.
When developing a security policy you must ensure that it does not prevent the business mission from being accomplished while at the same time, providing the best protection and recovery procedures to ensure continued accomplishment of the business mission. The process to perform this is called Assessment and will be the first step in the security policy development process. Besides the business mission, assessment is used to determine the data, information, and resources to be protected and what to protect it from, in other words the vulnerabilities in your network and the threats to the vulnerable assets. In order to perform a successful assessment, you will need a team consisting of members from various corporate

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

departments. The executive, administrative, and human resources departments can provide information on the business process and personnel requirements, which can assist in determining general access needs for day-to-day business functions. The legal department can ensure the policies and procedures protect the reputation and assets of the corporation and its partners as well as comply with federal, state, and local laws and statutes. All business functions are performed at a cost; as you develop your security policy, you should also develop a budget to implement and maintain the policy. The corporate Comptroller can assist with budget development and should be a part of the policy development team. As part of the assessment, you should review a cost benefits and effects analysis of outsourcing the corporate security program. Outsourcing of the corporate IT security requirements may be a viable solution if your corporations primary business function does not require a large IT staff. Out sourcing contracts usually include a security policy developed by the providing company in concert with the corporate security team. It is recommended that the outsourcing contract include a vessel for review of performance by the providing company. This requires a corporate security team, which will probably closely resemble the composition previously discussed.

**The Policy**

If the assessment determines out sourcing is the best method, then a policy should be developed that outlines the procedures agreed upon by the corporation and the providing company. If assessment decides against out sourcing, then a corporate security policy will be developed for all aspects of the security requirements.
First lets look at the definition of policies. On the Sans Security Policy web site (http://www.sans.org/resources/policies/) we find the following: “A policy is typically a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point-specific, covering a single area.” Additional reading in this area of the web site shows that the Network or Information Security policy will most likely refer to other policies, standards, and guidelines within the corporate policy structure. Why write an Acceptable Use policy if the Human Resources office already has one that may fit the IT requirements? What are the legal requirements of a Third Party Network Connection Agreement; maybe the legal department has what you need. Developing a Network Security policy is a complicated procedure and by building a team consisting of members from all corporate business functions, you are assured of reduced impact on business function and ready access to existing corporate documentation.

**What, Where, How, Basic Protection**

A good assessment will indicate what to protect, now comes the how and where. The corporation should develop a business computing equipment standard, which should be referred to by the Security Policy for capital equipment purchases. This will ensure that all IT assets, hardware and software perform at a minimum level or above and will provide for compatibility and standardization throughout your network. Purchasing hardware and software that is ISO 15408 [1] compliant will ensure that

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

the manufacturer has at least created a performance guideline and possibly provides compatibility results from an in-house testing program. Close scrutiny must be used when reviewing products based on this Common Criteria guideline as creative vendors can make their product look very good when it really isn't. Additional information on the Common Criteria ISO/IEC 15408 can be found in Ariffuddin Aizuddin's paper at http://www.sans.org/rr/standards/ISOIEC_15408.php. This paper also provides some links and reference to additional material about Common Criteria.

While attending the SANS GSEC Security Essentials course, a fundamental aspect of security was put in place with the introduction of the 'Security in Depth' principle more commonly called layered security. This involves the use of both hardware devices and software applications used at multiple depths or layers like the layers of an onion wrapped around the core, which is the data or hardware you are trying to protect.

The first line of defense is usually a perimeter defense, which may be provided by routers and/or a firewall structure, which can provide protection to hardware, applications, and data. This step requires the Security policy incorporate procedures for maintenance and management of all router and firewall configurations. The installation and configuration of routers and firewalls may be affected by other corporate policies, standards, and guidelines as well. An example would be the necessity of a DMZ to provide network access to third party partnering companies. Establishment of Remote Access Services (RAS) will require a policy or guidelines to implement and manage RAS, which would have to be incorporated into or referred to by the firewall policy and included in the new Security Policy. Router and firewall configuration will affect the operation of the corporate network and if configured incorrectly can result in unscheduled network outage. A team of IT professionals experienced in router/firewall configuration should review all configuration changes before the changes are implemented. The router/firewall policy should designate this team.

Because firewalls are designed to prevent intrusion, a method should be in place to verify the success or failure of the firewall structure. A common method to achieve this is through the use of Intrusion Detection Systems (IDS). IDS comes in two flavors, Network Intrusion Detection System called NIDS which monitor at the network level and Host Intrusion Detection System or HIDS which monitor at a particular host or computer such as a database server. Incorporating HIDS with NIDS helps to provide the layered defense mentioned earlier but will also increase the cost of network protection. This decision should be based on the determination of what you are protecting and the value of the loss or disclosure of the information.

Most applications "out-of-the-box" are configured with minimal security settings. Using security configuration guidelines from software vendors to harden your applications, in particular your operating system builds on the layered protection profile that is now in place. Care should be exercised when hardening an application to ensure availability after hardening.

With the proliferation of virus and Trojan applications and the resultant damage they do, a good security policy must include guidelines for the implementation and management of an antivirus application. The thought of virus and Trojans brings up

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

the point that assessment will determine the data, information, and resources to be protected and what to protect it from. Not all attacks come from outside the network and not all attacks are malicious. An employee who takes work home to process on his/her home computer may inadvertently introduce a virus or Trojan into the corporate network. The corporation should have a guideline established to address this issue and may include providing licensed copies of antivirus software to users that may be required to perform work at home. The IT security policy will refer to this guideline. If the guideline does not exist as other corporate documentation, the Security Policy will include a guideline to address the issue.

An Acceptable use policy will be included or referred to by the Security Policy to address use of internet/intranet/extranet assets by employees of both the primary corporation and partnering companies. The human resources department may include this policy as part of required reading for new employee check-in, if so then the existing policy should be reviewed and revised if necessary to include corporate IT assets. The existing policy will then be referred to by the security policy.

The corporate policy covering distribution of corporate owned and partnering company information and proprietary data will be a part of the security policy, either by inclusion or reference.

If the corporation provides RAS a policy will be required to govern methods of connection and establish access procedures. This policy may include or reference a Virtual Private Network (VPN) policy, which establishes requirements for connectivity through an Internet Service Provider (ISP). The RAS policy may also cover dial-in access use if it is not covered in a separate policy. Access to the network or assets on the network may require the use of Public Key Infrastructure (PKI) certificates. A policy should be established to govern Certificate Authorities, certificate issuance, storage and protection of private keys, and storage and dissemination of public keys.

A password policy will be created to define complexity, password security, and length of use, both minimum and maximum time between password changes. This policy may be part of a human resources policy governing all corporate password requirements and if so, should be referenced in the security policy.

Microsoft's newest operating systems as well as third party applications provide for data encryption to protect data from accidental or malicious distribution. The security policy will include an encryption policy to establish requirements and approved use of encryption. This policy ay be included as part of the PKI policy.

Application policies such as email services and web access will be developed to establish proper use. If an Application Services Provider (ASP) is used to host any application services, an ASP policy will be developed to ensure compliance with corporate security requirements.

An audit policy is part of any effective IT security policy. Properly configured audits will indicate what happened, when it happened and possibly how and by whom. Audit records can be used in prosecution efforts after a failed or successful break-in attempt if the audits are properly configured and the records are properly maintained. Chain of custody is a key point in any defense.

The security policy will also include a back-up policy. When backups are properly maintained and executed, the corporation will be able to quickly recover from any successful break-in. The back-up policy should include requirements for on-site and

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

off-site storage of back-up media. The events of September 11, 2001 attest to requirement of off-site back-up storage.
A configuration management policy will be created to establish configuration change procedures, authority, and documentation for the network configuration and may include the router/firewall configuration previously discussed. This policy will include establishing secure storage for the documentation.

**Conclusion**

The policies discussed in the preceding paragraphs are what I have learned should be considered as basic starting points when creating a new security policy for a network. No two networks are exactly alike so no single policy can cover all networks however all networks are subject to attacks from external, internal, or both sources and should be protected by security policy. The SANS Security Policy Project web site provides templates for the policies discussed in the preceding paragraphs as well as additional policies. The web site also provides links to other sources of policy templates. I have identified some additional links and will provide them in an Additional Information paragraph at the end of this document. Another source of good information can be found in RFC 1296 Site Security Handbook available from http://www.ietf.org/rfc/rfc2196.txt.
One thing to look hard at is the definition of a policy. From the SANS Security Policy web site, we read “A policy is typically a document that outlines specific requirements or rules that must be met….” The policies you decide are necessary for the protection of your network and data must have procedures developed to invoke the policies. Attempts to breach the security of networks occurs on a regular and continual basis which implies that security is a dynamic process and should be managed in a dynamic manner. The procedures should include a management process for review and modification of the policy contents on a regular basis.
The corporate IT security policy should include procedures for incident response. If the aftermath of an incident is cleaned up before proper incident response procedures are implemented, any possibility of recouping damages or seeking prosecution of the culprits will have been lost.
Knowing what tools and utilities that unscrupulous persons use to attack networks and becoming familiar with their operation and use will help the security specialist identify an attack, the method of attack, and possibly what assets on the network will be compromised if these devices are brought to bear on the network. This knowledge will also assist in preparing your layered defense to counter an attack.
Scheduled intrusion attempts, with prior approval of management can indicate weaknesses in your network defense. As mentioned in Scenario 1, any intrusion attempt can cause loss of communication and connectivity within your network and possibly loss of data. All scheduled intrusion attempts should be carefully planned and monitored to ensure no damage is incurred by your network or information systems.
I hope this paper has helped to relieve some anxieties for those of you new to the Information Security field and has provided you with the ability to determine a starting point.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

**Resources and Additional Information**

Best Practices
http://www.cisco.com/warp/public/126/secpol.html
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/howto/sechow.asp

More Resources
http://dmoz.org/Computers/Security/Policy/

Developing Policies
http://www.ietf.org/rfc/rfc2196.txt
http://wwws.sun.com/software/whitepapers/wp-security-devsecpolicy/
http://www.dc.fit.qut.edu.au/security/policy/10tips.htm
http://secinf.net/policy_and_standards/How_to_develop_a_Network_Security_Policy_.html
http://www.queeg.com/~brion/security/secpolicy.html
http://www.sans.org/resources/policies/
http://www.networkmagazine.com/article/sidebar1

Templates
http://www.sans.org/resources/policies/#template
Numerous sites are available on the web from which you can purchase templates.

**References**
Michele Guel “Proven Practices for Managing the Security Function”
http://www.sans.org/resources/policies/#primer
Security Policy, CERIAS http://www.cerias.purdue.edu/coast/intrusion-detection/policy.html
2002 CSI/FBI Computer Crime and Security Survey
http://www.gocsi.com/forms/fbi/pdf.html
Microsoft Technet
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/howto/sechow.asp
Incident Handling by Rik Farrow
http://www.networkmagazine.com/article/NMG20000515S0109
Developing Security Policies: Charting an Obstacle Course by Rosemary Sumajit
http://www.sans.org/rr/policy/course.php
SANS Security Policy http://www.sans.org/resources/policies/
The Common Criteria ISO/IEC 15408 – The Insight, Some Thoughts, Questions and Issues by Ariffuddin Aizuddin http://www.sans.org/rr/standards/ISOIEC_15408.php
Site Security Handbook http://www.ietf.org/rfc/rfc2196.txt

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.