Global Information Assurance Certification Paper

Protecting Information Assets: Review of an Information Security Policy
GSEC Version 1.4b, Option 1
Jeanette Whitney
January 17, 2003

Abstract

In this paper, I will examine several major policy areas contained in the comprehensive Information Security Policy of a large organization. I have not attempted to cover the entire policy in an effort to focus the paper on what I perceive to be the most significant areas. I will conclude my examination with recommendations for strengthening this policy based on the security principles of defense in depth, need to know, and least privilege stressed at the SANS 2002 conference in Washington, D.C.

Background

Information security has become increasingly more important over the past 25 years with the advance in network computer systems to store information electronically and to connect to the Internet. Internet connectivity, inherently insecure, allows businesses to survive and compete in today's market. However, because the Internet is based on open standards for ease of communication, Internet connectivity is not without risk of unauthorized access or industrial espionage. The growth of the Internet and its role in commercial business activity has created a challenge to minimize the risk and maximize the productivity of the enterprise.

Developing and implementing an Information Security Policy is essential to successful network security. "Although nearly every reference says that a good policy should be the basis for every successful security program, over 60 percent of companies do not have policies, or they have policies that are out of date," according to *Barman*.

The implementation of information security can be difficult across an enterprise network because of the range of security solutions and the variety of network configurations and topologies used. There are many security technologies available today, and choosing the right combination for your network and business requirements takes a great deal of planning. The problem is compounded as new technologies are brought online and new services or products are developed by the organization. The Information Security Policy must be flexible enough to accommodate changes in a timely manner. This can only be accomplished through regular review and periodic updates.

The first consideration when determining an Information Security Policy is the goal of the policy. A security policy is written to protect the organization's information assets. The policy outlines the boundaries of acceptable behavior by defining the rules for network use and procedures to prevent and respond to security incidents. Information security policies provide a high level outline that describes security in general terms, not in specifics. A well defined Information Security Policy is important to maintain consistency throughout the organization and to avoid liability when enforcing security rules.

An Information Security Policy is derived from a comprehensive risk analysis. The risk analysis involves identifying the assets and the threats that exist to those assets. Then, the

cost of eliminating the risk versus the cost of exposure to the risk, whether the cost of exposure is loss of information access, loss of competitive advantage, or loss of integrity, is weighed to determine the level of protection to apply to each asset. Each component of the Information Security Policy is based on the results of this analysis. The risk analysis report on which the Information Security Policy that I am reviewing is based, was not available for review; therefore, all recommendations in this paper may not be practical based on the current risk analysis.

Physical Security

Physical security is an integral part of an Information Security Policy. Physical security is probably the easiest security component to implement and the easiest to circumvent. If an intruder gains physical access to network equipment, the entire network may be compromised. Console access to equipment such as application servers, routers, and firewalls can result in opportunities for resetting and reconfiguring these devices. This may lead to loss of network services to customers as well as employees. Physical access to equipment could allow an intruder to use eavesdropping devices to gain access to sensitive corporate information resulting in a loss of competitive advantage and loss of market share. Physical security is essential in any Information Security Policy. Physical security incorporates plans for the protection of physical property, backup of critical data resources and the secure storage of the backups, as well as a comprehensive disaster recovery plan.

Physical Security Policy

The current Information Security Policy outlines controlled areas where more stringent restriction on physical and environmental security is required to protect information resources, such as computer rooms, telecommunications rooms, wiring closets, and computer operations areas. Access to areas requiring physical security is restricted to personnel whose job responsibilities require access. An access control list identifying the personnel who are authorized for physical access must be posted in the area. The access control list is reviewed on a prescribed schedule and updated accordingly. Based on the risk associated with unauthorized access to information resources and/or the sensitivity level of information available at some facilities, additional access control measures can be mandated. The control devices could include using biometrics, smart cards, tokens, CCTV alarms, mantraps, or lockable cabinets to supplement traditional facility locks and keys.

Identification badges are also part of the current Information Security Policy. Photo ID badges are mandatory for all persons in controlled access areas. These badges are required to be conspicuously displayed on the person at all times. Any attempted unauthorized access is subject to disciplinary action.

Network equipment, network servers, and mainframes must be protected against damage, unauthorized access, and theft. Essential equipment is required to be housed in a controlled area. All equipment is inventoried at regular intervals and labeled for asset management and physical protection. Those who use or have possession of portable equipment, such as laptop computers, notebook computers, palm tops, handheld devices, wireless telephones, and removable storage media devices, are responsible for their safekeeping. Personal digital assistants (PDAs) and handheld devices not issued by the company are required to be registered with an employee's direct supervisor. Visitors to

information resource facilities are required to check in with security officers and present PDAs or other handheld devices for inspection. Guest may be requested to surrender their devices for the duration of their visit.

Environmental security controls provide safeguards against lightning, wind, and building collapse. Redundant power feeds, redundant communications paths, and additional temperature and humidity controls are recommended for facilities hosting critical information resources. The potential for flood, earthquakes, or other natural disasters is evaluated for each facility. Surge protection, additional fire safeguards, and additional power (electricity) controls are required for critical information.

Physical security requirements are included in disaster recovery planning to ensure timely recovery and appropriate protection of information resources following the disaster. This plan incorporates contingency plans and facility recovery plans to address emergencies and disasters. These recovery plans for critical information resources are tested within 180 days of going into production and every 18 months thereafter.

To ensure the ability to recover critical information resources, redundancy planning and fault tolerant redundant systems are designed in the infrastructure. In addition, reliable backup procedures are required to be implemented using the defined backup media and maintaining the frequency schedule. The backup media is required to be stored at a secure location not subject to the same threats as the original media (generally off-site), and backup media must be maintained for as long as required by business. Electronic backup media or hardware on which electronic backup data is stored must be disposed of in a secure manner. Prior to disposal, all sensitive electronic data must be erased using a method that does not leave residual data on the media or equipment.

Evaluation of Physical Security Policy

My assessment of the overall Information Security Policy for physical security is good. There are, however, areas that could be improved. Much has been said about the physical access to controlled areas, but nothing has been said about the doors remaining locked at all times or the type of doors leading to controlled areas. It is my position that keeping the doors locked at all times requires no additional costs, requires only an awareness campaign, and can contribute to a more secure physical environment. The doors should be equipped with self-closing devices and should at no time be propped open. Although additional fire safeguards are mentioned in the current policy, use of sealed fire resistant doors would reduce damage in case of fire (Barman, 43-44).

The facility construction is covered sufficiently requiring redundant power feeds, temperature and humidity controls, surge protection, etc. However, there is nothing stating solid construction of barriers which could make the information resources vulnerable to unauthorized access. This should include solid walls and ceilings. This vulnerability is apparent by the Information Systems server room in my facility which is constructed with drop ceilings and a glass wall on one side. Although it is very attractive, it does not provide adequate security for one of our organizations most valued assets, our information resources.

The only policy regarding the security of portable equipment, such as laptop computers, is the person in possession of these devices is responsible for their safekeeping. This is a weak policy at best. Securing laptop computers has become a growing problem, and a more specific policy in this area is needed. "A 1998 FBI study found that 57% of network breaches originate form stolen computers," according to Kensington Technology. Guidelines should be developed defining the sensitivity level of data allowed to reside on laptop computers. The most obvious protection is to apply encryption to any critical data stored on the laptop. I would also include guidelines for securing laptops while in use in the office. For example, a laptop computer used in the office should be secured to the desk or to another immovable object using a security cable. If the laptop will not be used for an extended period of time, it should be required to be locked in a secure cabinet or safe. When traveling, if the laptop must be left in an unattended automobile it should be placed in the trunk and secured with a security cable. When it is impractical to secure the laptop, the employee should not let it leave his or her sight. Although not always convenient these suggestions will contribute to information security (Kensington Technology).

Access Control and Authentication

Access control and authentication is a major part of any Information Security Policy. This section addresses a broad range of critical topics such as securing the network perimeters, authentication, and remote access. Access control includes the login security policy which is sometimes referred to as the front gate. This is the point that the user must provide identification credentials to be allowed access to the network. This is a critical element in the overall information security policy.

Access Control and Authentication Policy

The current Information Security Policy requires that all network names and addresses be managed and approved by a central addressing authority. When appropriate, the controlling authority will conceal network addresses and provide translation of non-routable addresses. Network information is required to be protected and treated as "RESTRICTED INFORMATION." Access to network configuration information and addresses must be based upon the security principles of need to know and least privilege.

Perimeters are clearly defined boundaries that are established to securely control the traffic between corporate information resources and all other networks. All inbound or outbound network traffic is required to pass through appropriate access control devices, such as firewalls, before reaching corporate information resources. The corporate information security manager ensures the use of perimeter monitoring and may block the Internet Protocol (IP) address of a computer performing hostile reconnaissance or attacks against corporate networks. Other defensive measures to protect corporate resources require demilitarized zones (DMZs) to provide for the secure transfer of information between contractors, vendors, and the public. Only approved network services and protocols are permitted on the internal network, and any non-approved protocols and services must be disabled at the perimeter. All equipment connected to the network must meet current security hardening standards.

Remote access from a non-corporate site requires users or devices to authenticate at the perimeter or connect through a firewall. Modem access for information resources to and

from the corporate network must be approved in writing in advance by the information security manager and can only be established through centralized dial-in services. Strong authentication is required for personnel entering through dial-in, the Internet, or other non-corporate communications network. Any Virtual Private Network (VPN) solution used for business partner connectivity must be capable of filtering access to specific information resources, and the connection must allow monitoring. Any computing device connection to the corporate Intranet through a VPN must implement an approved personal firewall configured to corporate standards.

Accounts are established in a manner that ensures access is granted on a need to know and least privilege basis. Guest accounts are not allowed on corporate information resources. User accounts are configured to log the workstation off the network after a predetermined period of inactivity and should be automated where possible. The default standard period of inactivity is 15 minutes.

Logon IDs (or user IDs) are unique groups of letters, numbers, or symbols assigned to a specific person or information resource. Personnel using corporate information resources will be issued a logon ID in conjunction with the authorization process. If there are six unsuccessful attempts to log on to an information resource, the logon ID or account is suspended. Failed logon attempts are recorded for audit trail and incident reporting purposes. Computer logon IDs are suspended if not utilized for a preset period of time not to exceed 180 days. Logon IDs not used for a year are deleted. Personnel are required to identify and authenticate themselves to the network before being allowed to perform any other actions on the network.

The current policy requires all user passwords to consist of at least six characters and contain elements from three of the four following types of characters: English upper case letters (A-Z), English lower case letters (a-z), Westernized Arabic numerals (0-9), non-alphanumeric characters (special characters such as &, #, and $). Passwords must not contain the user's full name and must not be one of the past four passwords used for the account.

In addition, the following password recommendations are intended to enhance the password complexity and protect the password from attempted password cracking:

- Do not use family members names or other information easily discovered about the user.
- Do not use commonly used words such as words that appear in the dictionary.
- Do not use all the same characters or digits, or other commonly used or easily guessed formats.
- Use longer password conventions whenever possible (e.g., pass-phrases, or run-on multi-word strings).

Password expiration requirements are as follows:

- Prior to the expiration of authentication information such as passwords, the information resource will provide notification to the user.
- At least every 30 days, passwords for privileged or sensitive accounts (system supervisors, software specialists, system administrators, or vendor-supplied) must be changed.
- At least every 90 days, passwords for all other accounts must be aged and changed.

Information resources will deny access if the user does not comply with password selection or expiration criteria. The policy requires re-authentication by the user, as well as re-confirmation of the new password, at the time of an attempted password change. Initial passwords or re-set passwords, must be delivered in a secure manner (First Class Mail, encrypted delivery system, or hand delivered). Shared passwords are only acceptable if used for shared accounts. Passwords must never be written down and must be stored in an encrypted format. This includes passwords stored in batch files, automatic log-in scripts, software macros, keyboard function keys, or computers without access control systems.

Evaluation of Access Control and Authentication Security Policy

Although the Information Security Policy is thorough in this section, I did find some additions that could enhance login security. My first suggestion is to include the topic of login banners. There was no mention of restrictions applied to login banners used in the authentication process. The information displayed in login banners should be restricted from containing information about the system, such as operating system or company information that could be used by potential intruders. In practice, offending information is not used in the logon banner; however, a statement expressing this could be added to the policy to enforce this.

Passwords are often the weakest link in information security. The policy itself addresses some of the more common problems with passwords. However, limiting the reuse of passwords would strengthen the guidelines for password security. In the current policy, there are restrictions for expiration of passwords and that a user cannot use one of the past four passwords used, but no time specification. The policy can be amended to restrict users from re-using passwords for a specified period of time (at least 24 months).

Acceptable Use Policy

The acceptable use policy should present the overall user responsibilities of Information Security Policy in clear and concise language. Employees must be informed of exactly what those acceptable uses are and what penalties befall the user for misuse. In the following section I will review two areas of the acceptable use policy for my employer: the Internet policy and email policy.

Internet Security

Corporate Internet access can be a major security vulnerability. Filtering can be done at the perimeter on devices such as routers and firewalls to allow or deny traffic based on protocol, port, and source or destination IP addresses as presented in the access control section. If access is permitted from inside the corporate network to the Internet, the decision must be made as to how much access is needed to perform job duties and how much will be allowed. The policy relies on the user following the rules set forth in the Information Security Policy. User activities can be monitored to ensure that policies are followed and disciplinary action can be taken where misuse is detected.

Acceptable Use of the Internet

The current Information Security Policy provides Corporate Internet access to facilitate and conduct corporate business. Occasional and incidental personal Internet use is permitted if it does not interfere with the work of personnel or the Corporations ability to perform its mission and meets the conditions outlined in the policies and procedures manual.

Prohibited activities when using the corporate Internet include, but are not limited to, the following:

- Browsing explicit pornographic or hate-based web sites, hacker or cracker sites, or other sites that the corporation has determined to be off limits.
- Posting, sending, or acquiring sexually explicit or sexually oriented material, hate-based material hacker-related material, or other material the corporation has determined to be off limits.
- Posting or sending sensitive or business-controlled sensitivity information outside the corporation without management authorization.
- Hacking or other unauthorized use of services available on the Internet.
- Posting unauthorized commercial announcements or advertising material.
- Promoting or maintaining a personal or private business.
- Receiving news feeds and push data updates, unless the material is required for corporate business.
- Using non-approved applications or software that occupy or use workstation idle cycles or network processing time.

Evaluation of Acceptable Use of the Internet

The policy itself adequately lists prohibited activities but is dependant on the user having knowledge of and following the rules outlined in the policy. Users should understand that Internet communications are not always secure, and care must be taken not to disclose private information. There should be guidelines developed to ensure employee awareness of acceptable use of the Internet and the right of the organization to monitor and audit traffic through the corporate Internet connection. The organization can mandate that all

employees sign a waiver acknowledging they have read the policy and agree to as a condition of employment. This would be critical and could prevent an employee lawsuit if enforcement of the policy required disciplinary action.

Email Security

Email has changed the way we communicate in business as well as our personal lives. The ease of use and convenience make it a popular means of communication. Improper use of email can be annoying with chain letters and unsolicited mail; and it can even be catastrophic with viruses and malicious code attached to email. Establishing an acceptable use policy for email is an essential part of an Information Security Policy. As with the Internet policy it relies on the user following the rules set forth in the Information Security Policy. User activities can be monitored for traffic, content, and scanned for malicious code. This ensures that policies are followed, and disciplinary action can be taken where misuse is detected.

Acceptable Use of Email

Access to the corporate electronic mail (email) system is provided to personnel whose duties require email to conduct business. Corporate email services can be accessed from corporate information resources. Since email may be monitored, all personnel using corporate resources to transmit or receive email will have no expectation of privacy.

Occasional and incidental personal email use is permitted if it does not interfere with the corporate ability to perform its mission and meets the conditions outlined in the policies and procedures manual. However, while they remain in the system, personal messages are considered to be in the possession and control of the corporation.

The use of corporate information resources to check personal email accounts, such as Hotmail, Yahoo, Excite, MSN, etc., is prohibited. Other prohibited activities when using corporate email include, but are not limited to, sending or arranging to receive the following:

- Information that violates state or Federal laws or corporate regulations.
- Information designated as sensitive information unless encrypted according to corporate standards.
- Unsolicited commercial announcements or advertising material.
- Any material that may defame, libel, abuse, embarrass, tarnish, present recipient, the sender, or any other person.
- Pornographic, sexually explicit, or sexually oriented material.
- Viruses or malicious code.
- Chain letters, unauthorized mass mailings, or any unauthorized request that asks the recipient to forward the message to other people.

Encrypting email or messages must comply with the following:

- Encryption software and methods must be approved by management.

- Encryption solutions must either support key recovery or keys must be registered with authorized personnel.
- Recovery keys or other similar files or all encrypted email must be placed in a directory or file system that can be accessed by management prior to encrypting email.
- Recovery keys or other devices needed to decrypt email must be provided when requested by authorized corporate management.
- Keys may not be escrowed in customer product offerings unless specifically requested in writing by the customer and approved by the executive sponsor.

While system administrators and other personnel may have unrestricted access to data, email, and similar services must receive management approval prior to decrypting or reading the email of other employees. Generally, such approval is based on suspected infringement of corporate policy.

Evaluation of Acceptable Use of Email

An acceptable use policy for email faces the same problems as the acceptable use policy for the Internet. Unless the user is aware of the rules, the policy is ineffective. There should be guidelines developed to ensure employee awareness of acceptable use of the email, and the right of the organization to monitor the handling of email. An employee awareness program regarding the acceptable use policies and procedures might be integrated into the employee orientation program for new hires and reviewed annually when reviewing benefits packages for existing employees.

The organization is currently limiting the size of each email to 4 MB, but this size limitation is not documented in the policy. It appears that this size restriction is used more to manage resources than information security purposes.

Virus Protection

In the network industry today, computer viruses are as well known as human viruses and act in much the same way. A computer virus attaches to a computer program which infects that system and can be replicated by a user action such as copying to floppy or emailing. Worms are another form of virus that has the ability to self-replicate to other programs enabling it to infect other computers in a networked environment. This type of attack is one of the most dangerous forms of network abuse and can be devastating in a corporate network causing lost productivity and lost information resources.

Virus Protection Policy

The current Information Security Policy for my organization requires that all information resources within the corporate network have active virus protection software installed and enabled. Virus protection software runs on workstations, laptops, and removable media prior to the sharing of files. Unauthorized personnel are prohibited from modifying the configuration of virus protection software after installation. All application software is protected in such a way that an error message will be generated if there is an unauthorized

attempt to modify the software and all activities involving modification of software are logged. Virus protection software and signature files are required to be periodically updated or can be immediately updated when a new threat is perceived.

All software applications, data files, or any other type of digital media are required to be tested to identify the presence of computer viruses and other malicious code prior to distributing. To ensure perimeter security, security information services will conduct scans for malicious code on the firewalls, FTP servers, mail servers, Intranet servers, Internet application protocols, and other information resources as necessary.

Evaluation of Virus Protection Policy

The virus protection policy establishes that a reasonable virus protection policy is in place. There is no virus protection software that will provide one hundred percent protection. The possibility of getting a virus that the existing virus protection software is not capable of finding always exists. This stresses the importance of requiring periodic updates or immediate updates when a new threat is perceived. The statement that prohibits an employee from sending or arranging to receive viruses or malicious code is mentioned in the acceptable use of email section of the policy. The addition of a strong policy statement to reflect the penalties for involvement of an employee in this type of destructive activity would significantly enhance the effectiveness of this policy section.

Encryption

Encryption is the primary means for providing confidentiality services for information sent over a computer network. In the past, encryption was primarily associated with the military or government using forms of encryption to keep secrets from foreign governments. Cryptography dates back through the millennia and has been used for the sole purpose of keeping secrets. Information sent in plain text (without encryption) over the wire is vulnerable to eavesdropping and information theft. Encryption technology is now common practice in the information security world to provide confidentiality and prevent attackers from stealing sensitive information.

Encryption Policy

The policy presently states that information resources storing or transmitting sensitive information must have the capability to encrypt information. Sensitive information stored in non-secure locations or transmitted across un-trusted networks must be encrypted. Additionally, it may be recommended that sensitive information stored in a secure on-site or off-site location be encrypted. The minimum encryption standard is triple Data Encryption Standard (DES) with a 128-bit encryption key or the Advanced Encryption Standard (AES).

The policy also states that key management must be rigorous and disciplined. Encryption keys must be treated as sensitive information, and access to keys must be restricted on a need to know basis. If keys are generated and stored, the information resource must provide secure key storage that is resistant to compromise through a logical or physical disk. If hardware-based key generation and storage is used, the key must be stored in such a way that it cannot be retrieved in clear text. If key recovery is supported, access to the key must be limited to authorized personnel. The capability to enforce the immediate

revocation of user accounts and the associated key(s) must be available. Any information resource used by the encryption process must be thoroughly erased, with no residual data exposed when released.

Evaluation of Encryption Policy

The encryption section of the Information Security Policy covers handling of encrypted data and key generation and management issues. However, since encryption standards are controlled by government, a statement mandating management to actively solicit the most up to date encryption regulations would ensure the company complies. Government agencies or any organization contracting with the federal government must meet current published government encryption standards.

Compliance and Monitoring

Monitoring is used to ensure appropriate use of corporate resources and improve security by protecting information resources from attack. When monitoring employee activities, it is important to consider any legal issues with regard to privacy. In most cases, it is legal to monitor; however, the employee has the right to know they are being monitored. This is another area where employee awareness is critical. Monitoring is an important part of the Information Security Policy with statistics showing that a large percent of security violations are initiated from inside the corporate network.

Compliance and Monitoring Policy

The security control officers have the legal right to monitor and audit the use of its information resources as necessary to ensure compliance with corporate service policies, procedures, standards, and guidelines. The audit process is a review of records and activities performed that ensure compliance with established policies and procedures and will recommend changes when security deficiencies are found. The activities performed by a user on corporate computer resources are subject to audit or monitoring, and any detected misuse of computing resources may be subject to disciplinary action up to and including removal, termination, and criminal prosecution. Use of corporate information resources constitutes permission to monitor that use.

The current policy states that the monitoring of information resources may include, but is not limited to, the following:

- Network traffic
- Application and data access
- Keystrokes and user commands
- Email and Internet usage
- Message and data content.

Requests for monitoring network traffic, application, data access, keystrokes and user commands, and email and Internet usage must be directed, in writing, to the corporate

information security officer. Requests for monitoring message and data content must be directed to the chief privacy officer in writing.

If threats to the corporate infrastructure, network, or operations exist, the corporate information security officer is authorized to take appropriate action, which may include viewing and/or disclosing data in order to protect corporate resources or the nation's communications infrastructure. The corporate infrastructure is secured through incident detection using perimeter virus scanning and intrusion detection services, performing vulnerability analyses and infrastructure monitoring.

Where possible, information resources must display an authorized corporate warning banner on the workstation screen before an individual is given access to the corporate information resources. The banner identifies the computer as a corporate computer system protected by criminal code, provides notification of monitoring, and will be followed by a pause requiring manual intervention to continue.

Evaluation of Compliance and Monitoring Policy

The compliance and monitoring section establishes a right to monitor and includes control statements describing what controls are in place. The policy should address the examination of log files. This would include who is responsible and the frequency of examinations. The monitoring software is usually the first to detect a violation and should be configured to alert the appropriate personnel when a violation occurs. This section should also include the penalties involved when policies are violated. The policy should include statements that cover attacks from within the corporate network as well as from an external intruder. This ensures consistency and will establish clear guidelines when enforcing these penalties.

Conclusion

The purpose of this paper is to review, evaluate, and recommend proposals that would strengthen selected areas of the current Information Security Policy for my organization. As expected, the Information Security Policy for this national enterprise was comprehensive and exhausting to review. I recognized the most significant deficiency is not inherent in the policy itself but comes from the lack of awareness of the policy by the employees of this organization. I base this conclusion on the fact that I have been employed by this organization for a number of years and have been unaware of several specific policy areas. A formal training program accomplished through an orientation process or annual review would be a good place to start increasing employee awareness. This training should include guidelines for password selection, login procedures and safe practices to prevent password theft, and unauthorized access. It should also include acceptable use for the Internet and email, right to monitor policies, and possible disciplinary actions for non-compliance to policy. The success of the policy depends on the support of management and the awareness of the employees.

Another area that would strengthen the current policy is improving the enforcement of the policy. Again, the policy itself appears to outline adequate security measures in most areas. However, based on my knowledge of the organization, the enforcement of the policy regarding the internal user is lax. The policy should define what disciplinary actions should

be taken based on the type of violation and follow through with the course of action when an incident is detected. When the policy is not enforced properly, the policy becomes ineffective.

I propose a complete review process should be performed at regular intervals (at least annually). This should be defined in the Information Security Policy. The review should be performed by a committee with representatives from management, information systems, human resources, and from the corporate legal department. This review should include information gathered from a risk analysis or audit. The committee should also review the impact of the security policy on network performance. Some policies may dictate more security initiatives than necessary and degrade performance unnecessarily, while other areas may need more security that is currently required. Each member of the committee should provide recommendations to improve the Information Security Policy and protect corporate information resources.

A computer network is never one hundred percent secure; however, developing and implementing a solid Information Security Policy is the first line of defense in network security. Successful implementation of Information Security Policy can be a difficult task and takes considerable planning. Diligence is required to support the continuing maintenance of the security effort. Every employee in the organization has a responsibility to maintain security of corporate information resources. This is only possible with systematic employee awareness training programs that produce a well informed work force.

References

[1] Holbrook, P. and Reynolds, J. "Request for Comments: 1244." July 1991.URL: http://www.ietf.org/rfc/rfc1244.txt?number=1244

[2] Sun Microsystems. "How to Develop a Network Security Policy." December 2002. URL: http://wwws.sun.com/software/whitepapers/wp-security-devsecpolicy/

[3] Fraser, B. "Request for Comments: 2196." September 1997. URL: http://www.ietf.org/rfc/rfc2196.txt?number=2196

[4] Singapore IT Security Techno Portal. "How to Develop a Network Security Policy." October 2002.URL: http://secinf.net/info/policy/netsec1.htm

[5] Eckhouse, John. "Snooze and Lose When it Comes to Security." October 2002. URL: http://www.optimizemag.com/issue/012/gap.htm

[6] Queensland University of Technology. "Feeling Insecure, 10 Tips for Creating a Network Security Policy." October 2001.URL: http://www.eweek.com/article2/0,3959,112398,00.asp

[7] Cisco Systems, "Network Security Policy: Best Practices White Paper," Document ID: 13601. April 2002. URL: http://www.cisco.com/warp/public/126/secpol.html

[8] Kensington Technology Group. "Why is a Laptop Security Program Important?" December 2002. URL: http://www.computerlocks.com/tools/too_1019.html

[9] Barman, Scott. Writing Information Security Policies. Indianapolis: New Riders 2002.

[10] Bragg, Roberta. Certified Information Systems Security Professional. Indianapolis: Que November 2002.