Global Information Assurance Certification Paper

Implementing a Secure Information Policy and Procedures

By

Sharon Buggele

October 23, 2003

GSEC Practical Assignment version 1.4b

Option 1

Implementing a Secure Information Policy and Procedures

Abstract:

In an organization network security is an important issue, but it is often overlooked due to the fact that organizations do not have a full understanding of what they should be doing or how to go about it. The availability of information on this topic regarding its guidelines and procedures are obtainable from many sources. The problem resides in the awareness of the first intrusion and then the deployment afterwards of policies and procedures within the organization to prevent future intrusions.

The definition of a security policy is, “In business, a security policy is a document that states in writing how a company plans to protect the company's physical and information technology (IT) assets. A security policy is often considered to be a "living document", meaning that the document is never finished, but is continuously updated as technology and employee requirements change. “ (SearchCRM.com) A security policy usually includes a users policy that describes the responsibilities and roles of the users with regards to network usage and security. This in turns educates the employees about the protection of an organization’s assets.

Introduction:

As computers and networking have become more ubiquitous, security is no longer a backroom issue. It's everyone's concern. Security depends on balancing cost and risk through the appropriate level of technology and policy. Too little security can be dangerous and costly. In a recent survey by CIO Insight in August 2003, the vast majority of more than 600 IT executives were polled and less than 10% felt that their organizations security was adequate. In the same survey 34% felt they were enforcing and doing their security policies. While 65% answered that they did not meet goals when it came to education. But the survey suggested that the level of concern with security dropped since the September 11 attacks. The question to ask, are they living in a dream world or have they prepared adequately for security threats? How do you decide the appropriate level of security for your enterprise?

The most popular misperceptions are often considered as network attacks done by mischievous teenagers or social misfits. There are facts that indicate that these members of this group represent a small number of the widely diverse number of criminals who cause cyber-crimes inside and outside the organization according to (KPMG, 2000). The list of internal attackers includes dissatisfied current employees who work alone or with other insiders of the organization. Also included in this list are disgruntled ex-employees or competitors employees

who wish to do harm or gain a competitive edge. A cyber attack can cause four damaging affects to an organization, no matter who the perpetrator is:

- Result in the theft of an asset;
- Corrupt an asset;
- Destroy an asset; or
- Deny access to an asset.

In order to prevent the destruction, manipulation or misuse of an organizations data and resources, the organization need to implement a secure informational policy. In developing policies and procedures we will be using a policies designed by the National Center for Educational Statistics:

1. Outline security and privacy policies for users
2. Outline authentication policy for users
3. Securing network hardware
4. Securing operating system
5. Securing software
6. Securing the network
7. Network monitoring
8. Planning for disaster recovery
9. Staying informed of new technology

1. Outline Security and Privacy Policies for Users:

People play an important role in the awareness training of security, not only from a personal perspective but from a technical perspective. Mark B. Desman stated, "Information security is a people, rather than a technical, issue.'' Therefore, they will need to enlist the cooperation of the people using any information technology equipment. The technical tools, access control software, firewalls, hardware identifiers or any other hardware and software measures, are directed at controlling human access to systems assets.

The consistent error that information technology professionals have made since the days of punch cards and pure mainframe processing environments are that they think that the new technology will provide all the answers. What they are missing is that what the input of the process is for the people and the output is used by the people. In today's environment we give users control over the local and corporate environment, which permits them to carry corporate assets to and from the location.

User's both outside and inside the organization must be educated in the safe utilization of accessible information. The users must be made aware that the granted privilege is a responsibility and that they are responsible for it. Users must also be made aware of that all the hardware and the software will not

protect them from external attacks, that are why communication is such a vital single point of a information security policy.

The process of the language used to make users aware of the security policy and procedure must be spoken in a language that the users understand. User's come from a wide variety of backgrounds and work environments which can cause conflicts in understanding the jargon of the information technology field. Therefore you must learn to speak their language in order to communicate properly and effectively with them. For-example a copy of a Privacy Policy on an organizations website may be written like: *If we decide to change our privacy and/or security policies, we will post those changes on this page so that you are always aware of what information we collect, how we use it, and under what circumstances we disclose it.* This form of dialogue is very important not only for the employees of the organization but also for the Information Technology teams who are maintaining the networks.

Communication with the user must provide a purposeful concept, which will allow the user to identify with it in the direction necessary for deployment. The final point in the communication with the user is that you must get it to them in a timely manner and in correct format. This is very important so that they understand the issues and importance of specific areas. Their participation is vital in the success of the overall program.

The most import element of a company's computer user's policy is the statement that "company computing systems are provided as tools for business and all information created, accessed, or stored using these systems are the property of the company and subject to monitoring, auditing or review. The computer policy should protect proprietary information, prevent copyright infringement, and make sure that some employees were not using hostile work environment for other employees. Employees should also include statements that spell out the consequences for violating company computer use policies. Although establishing computer use policies is critical, it is equally important to make sure that the policies are disseminated. Below in **Table 1** are examples of the key elements of a computer user policy to be followed.

Table 1: The key elements of computer user policy
Policy element
Monitoring use of proprietary assets
Establishing no expectation of privacy
Improper employee use
Allowable employee uses
Protecting sensitive company information
Disciplinary action
Employee acknowledgment of policy
Source: GAO's analysis of recommended computer-use policies.

2. Outline Authentication Policy for Users:

Users of the system fall into a variety of categories ranging from a guest to a system administrator. The policies for these users will not all be the same. For-example a guest password may be public and static. This would limit the account scope to access only certain areas. On the other hand a system administrator's password would have different parameters, due to the complexity of the account. That would take into the practice of the built-in system administrator password, which would be known by a select few of individuals. The next categories are the system administrators, whose user-Ids have administrative privileges, which would also include Enterprise Administrator, and Domain Administrator. The final group would be the operators, such as the Print operators, and Back-up Operators.

All of the above accounts must have adequate password protection, if not they open a virtual door to hackers. A common scenario is one in which an account's user name and password are the same – know as a "Joe" account. Weak passwords can be prevented by setting password complexity requirements in the operating systems. The enforcement of strong password rules, such as passwords, longer than eight characters, that are revised monthly, and includes numbers and characters. Passwords must be unpredictable and the policy that protects them should be as unpredictable as possible.

Another form of prevention is to allow only three log-on attempts before a 15-minute-or-so lockout occurs. If the password rules are difficult to remember, then the Information Technology department will find sticky notes pasted on employee monitors to help them remember passwords. User should be instructed about their responsibility to keep passwords and system infrastructure in total confidence.

To prevent unauthorized access to accounts that organization should have a password-protected screen saver that kicks in after 10 minutes of inactivity. Peer-to-peer network like the file-sharing services, such as iMesh and Kazaa, have no place in an organization. Apart from using bandwidth and the potential copyright violations they also include file-sharing properties that can expose the network to outside vulnerabilities. Formal policies around these areas such as file sharing services and remote access help employees understand there responsibility and to recognize and report suspected problems.

3. Securing Network Hardware:

Electronic security is important but there are other areas to consider, including physical security and operational training. Physical security such as hardware security is crucial. This includes the physical protection of equipment (e.g., computers, printers, monitors, etc.) from both theft and damage. Different types of hardware require different types of protection. Servers and related

equipment should be placed in a secure room with limited access. This room should have proper environmental conditioning and fire protection equipment. This proper security deters theft of property, effective hardware security bars unauthorized access to the server. The principles of security-technology infrastructures become moot if an intruder can simply walk in and access critical systems.
Further policies to insure hardware security include:

- Centralized location for the storage of hardware with lockable entry;
- Proper fire protection system exist;
- Maintain proper environmental controls;
- Provide adequate electrical power;
- Provide emergency source of power;
- Monitor the room environment and electrical systems;
- Use network monitoring and utilities that display log data traffic to detect the installation of unauthorized hardware and/or software applications.

4. Securing Operating Systems:

The operating system security consists of limiting access to network resources, as files and directories, centralized applications, network printers and other components. The network access should be determined by personnel specific task related to ones work. An appropriate policy for operating system security is a baseline denial of access to all components for all personnel, with explicit access privileges granted on a case-by-case basis. User's login credentials will identify the role(s) and the profile of the user will "describe" the access parameters to the operating system.

Some access-related security measures that should be implemented are as follows:

- Disable guest accounts;
- Change default passwords;
- Force frequent user password changes;
- Allow only non-dictionary passwords;
- Deny access by default;
- For ease of administration, control access based on groups, profiles, policies;
- Require administrator access through a different login mechanism, *not* through the normal user login.

5. Securing Software:

Security software will help limit copyright infringements, assist in proper licensing of software and will ensure that only authorized personnel have access to the software installation media. Software installation media should be stored in a centralized location with proper documentation of the number of licenses and number of installations. These media should be protected from harsh environmental conditions, such as electrical and magnetic fields, excessive heat, and moisture.

Some recommendations for software security are as follows:

- Store software media in a locked cabinet within a proper environment;
- Allow access to applications through the use of network security settings to those groups /users that require access;
- Implement a software-auditing package;
- Standardize applications across the organization;
- User virus-scanning software with frequent definition updates;
- Use spam prevention software to prevent unauthorized entry to email.

6. Securing the Network:

The same security procedures in place for server hardware apply to equipment that supports the network, including switches, firewalls, hubs, routers, cabling, etc. Network equipment should be installed in an environment with proper ventilation and power requirements, and protected from unauthorized access.

Some basic precautions for securing network equipment are as follows:

- Limit access to network equipment to authorized individuals;
- Do not allow users to install unauthorized network equipment;
- Ensure proper cabling and cable protection

7. Network Monitoring:

Maximization of network monitoring takes place by the implementation of an intrusion detection system. These systems watch IP data packets as they transit the network outside the firewall. They monitor distributed denial of service (DoS) attacks, attempted port scans and other intrusion attempts. Intrusion detection protocol should include the following tasks:

- Enable port monitoring outside the organization firewall;
- Review intrusion detection system log files daily;
- Configure blocking on the router

8. Planning for Disaster Recovery:

In the development of an Information Technology policy for an organization the backup and recovery of data is often overlooked. Another common problem is that organizations with a backup plan fail to do scheduled backups and recovering testing. It is imperative that an organization's be committed to the development, implementation and maintenance of a disaster and recovery program.

Part of a successful disaster recovery plan is insuring that hardware has redundancy built into it. By using clustered servers, data can be backed up on different servers thereby increasing the redundancy of the servers. An organization that is heavily data dependant can arrange to have a remote backup to keep data backup offsite. Offsite backup also allows for operations to be transferred in case of physical damage to the building e.g. fire or damage to the site.

9. Staying Informed of New Technology:

With over 60,000 viruses in circulation it is imperative that an organization have virus protection in place. With the correct installation and frequent updates the virus protection should prevent any data corruption due to viruses. Email servers should scan for viruses and take appropriate action before been delivered to a user's inbox. Desktop and server virus protection protect users and data from malicious code. Centralized management and scheduled updates makes updating of servers and desktop more automated.

In the exchange of data across the internet encryption of that data has become important. To insure the privacy of data and to allow for the correct authentication organizations can purchase RSA public key for authentication and data encryption.

The organization needs to have an email policy in place so that users know the company stance on using e-mail. According to Brightmail Inc, a major vendor of anti-spam software, spam accounts for nearly 40% of all e-mail traffic in the US. With the proliferation of spam future networks will be bogged down in band-width and processing time handling the influx of spam. It would be an organizations interest to stay ahead of the development of new anti-spam software to detect and correctly process e-mail into spam.

"Protecting enterprises on the move in today's mobile environment, security is more important than ever." stated by Pointsec Mobile Technologies. Access to critical information at any location for a particular organization creates opportunities, but also poses new security threats. These threats are visible by the information being reported by several security organizations. The above is due to the facts that the data and information has become more accessible,

because it becomes more exposed. Nevertheless with the right solution, the proposed threats can easily be neutralized, allowing organizations to safely deploy today's mobile devices without compromising security.

Conclusion:

Just as a company has procedures and policies to protect it's assets and employees from harm, so too must implemented a set of policies and procedures to protect it's informational infrastructure. With the growth of external threats from viruses and spam as well as the rise in technology usage internally, the importance of security policies and procedures is now more than ever a priority with the organizational structure. The success of a security policy and procedure within an organization is dependant on user education about their roles and responsibilities with regards network usage and operations. The policy and procedure awareness plan makes identification with the organization to satisfy and perform the needs required by the users which enhances the security outlook of the organization.

References:

Chapter 6: Maintaining a Secure Environment. National Center for Education Statistics. 16 Oct. 2003 <http://www.nces.ed.gov/pubs2003/secureweb/ch_6.asp>.

Desman, Mark B. "The Ten Commandments of Information Security Awareness Training." Security Management Practices. Jan. 2003: 39-44. 01 Oct. 2003.

Dowland, P. S., S. M. Furnell, and M. Gennatou. "A prrototype tool for information security awareness and training." Logistics Information Management 15 (2002): 352-357. 14 Sept. 2003.

Madnick, Stuart E. "Management Policies and Procedures Needed for Effective Computer Security." Sloan Management Review (1978): 61-74.

Pointsec Mobile Device Security. 14 Oct. 2003 <http://www.pointsec.com/core/default.asp>.

SearchCRM.com. SearchCRM.com. 16 Oct. 2003 <http://searchcrm.techtarget.com/gDefinition/0,294236,sid11_gci548251,00.html.

Shipley, Greg. "Are You Vulnerable?" Network Computing. 26 June 2003: 1-7. 02 Oct. 2003.

Stamper, Jason. "Policing the policy." CBR Research. 29 Oct. 2002: 5-6. 11 Oct. 2003 <http://www.computerwire.co.uk>.

Warren, M. J. "Security practice: survey evidence from three countries." Logistics Information Management 15 (2002): 347-351. 13 Oct. 2003.