Global Information Assurance Certification Paper

Considerations for an Acceptable Use Policy for a Commercial Enterprise
David P. Ehinger
22 November 00

Policies, policies, policies

If you have attended any reputable computer security training seminars lately you are probably getting tired of hearing about policies. But policies are the high cover that allow the computer security professional to effectively operate in an enterprise where the ultimate goal is to produce a product at a cost that allows the company to successfully compete in the marketplace. This means that cost of providing computer security will always be involved in trades against other financial demands of the company.

In addition, no matter how large the computer security budget may be, the purchase and installation of various hardware and software security solutions will never completely solve the problem. Security system vendors will always be at least one step behind the changes in the business environment and users will always find ways to circumvent installed systems.

Recent studies by the FBI Computer Security Institute have shown that 70% of network attacks are by outsiders, but these same studies show that 75% of the dollar losses to businesses are from insider attacks [1]. An acceptable use policy is a first step in restricting the insider threat as it defines the expectations the company has of it's employees as they utilize the company's systems.

In developing the policy the IT security professional should coordinate with the company legal and human resources staffs. The legal staff can help to insure that the policy is legal and enforceable and the human resources staff will be called upon to conduct any employment related actions based on violations of the policy. Therefore the input from these two groups is paramount in developing and successfully enforcing an Acceptable Use Policy. In addition the IT Security Professional must insure that the policy is consistent with the company's overall security policies and is fully supported by the company's senior management.

Considerations

The following paragraphs cover some of the most common considerations companies may need to include in an acceptable use policy. Each company's needs will vary depending on the type of business the company is in and the makeup of their employee population and the configuration of their information systems.

Applicability and Purpose. A clear statement of applicability and purpose can go a long way towards enforcing compliance, particularly if the organization will be giving systems access to personnel who are not direct employees of the organization.

Changes. Nothing is a constant as change and this holds true of your acceptable use

policy. As technology changes and new threats to the business emerge, there will be changes to your policy required. The company should include in the policy the method for communicating these changes to employees.

General Principles. It is good idea to include up front in the policy a statement of general principles regarding usage of the organization's systems. Are the systems to be used strictly for business purposes only or is some amount of personal use to be tolerated? If personal use is to be tolerated, what are the limits?

Employee Monitoring. The company may wish to state their intent to monitor in the acceptable use policy. In some jurisdictions this morning may be required, in others it may be optional. The policy should state what the purpose of the monitoring is and how the results will be used. Companies should be cautious as some activity such as union activity cannot be monitored.

Adult activity. It is a good idea to include a strict prohibition against any adult activity such as visits to adult Internet sites or the distribution of adult content using the company's e-mail system.

Hostile workplace. In addition to adult activity there are other activities that can contribute to a hostile work environment and leave the company open to legal challenges. These may include harassing jokes, threats, and other items that have no place in a productive work environment.

Hacking. Companies should include a clear prohibition against using the organizations systems to attack or otherwise compromise systems the user does not have legal access to.

Safeguarding systems and data. The company may want to make it clear that the user has a responsibility to properly protect systems and data the user is given access to. It is a good idea to require users to check any files brought into the company for viruses and malicious content prior to opening the file. A prohibition against introducing non-business related files should also be considered. In addition users should be cautioned concerning the distribution of data owned by the company to outside persons or organizations.

Companies that deal in highly technical areas may find that their data is export controlled and may require the proper documentation prior to release to foreign persons. Users need to be cautioned that this requirement applies to electronic transmission of data as well as physical transmission.

Many companies require the use of an automatically activated password protected screen saver when there is a lack of user activity for a predetermined period of time. This provides some protection to the network and the user as someone other than the logged in

user cannot easily use the logged in computer. In this same vein users should be required to log out when they will be gone from their workstation for extended periods of time or when they leave for the day. Some modifications to this requirement may be necessary for certain systems where the logoff would cause interruptions to an ongoing process and where the workstation lock provides a level of security similar to the network login process.

Protection of user ID and passwords. A prohibition against sharing user IDs and passwords should be included. Without such a prohibition the organization may find it difficult to clearly trace activity back to a specific user.

Modems. Organizations need to determine how the requirements for modems in the workplace will be handled. Even in this day of web-based everything the requirements for modems has not been completely eliminated. When they are necessary they should be considered a deviation to policy with a defined approval scheme.

Telecommuting Employees. Organizations are promoting telecommuting to allow their employees to work from home, while they are on travel, or while visiting a client site. Depending on the environment the telecommuter may not have full access to all network functions. The following paragraphs discuss some of the telecommuting hazards that need to be considered when writing the acceptable use policy.

Many organizations have implemented web-based e-mail to allow employees to easily access their e-mail from any location where Internet access is available. While this method of access provides the maximum availability it also opens the business up to a number of potential risks. If the e-mail is accessed from a public kiosk what control does the user have over the storage of temporary files on that kiosk? How certain can the business be that the kiosk operator has sufficient controls in place to insure the privacy of the communication and the deletion of the appropriate files when the user is finished?

Organizations that promote telecommuting must also evaluate the equipment that will be used by the telecommuting employee. Allowing the telecommuting employee to utilize individually owned equipment places the network at additional risk. The telecommuting employee likely also uses their individually owned equipment to access the Internet for personal reasons at their home. The threats to the company network from private Internet activity abound. In 1998, the National Institute of Standards and Technology (NIST) categorized and analyzed 237 computer attacks that were published on the Internet [2]. This sample yielded some interesting statistics that should get the attention of every security professional:

- 29% of attacks can launch from a Windows host
- 20% of attacks are able to remotely penetrate network devices
- 3% of attacks enable Web sites to attack those who visited the site
- 4% of attacks scan the Internet for vulnerable hosts

- 5% of attacks are effective against routers and firewalls

Therefore the business network may become a target for trojans, viruses, and worms loaded on the user's home computer due to otherwise innocent Internet activity. The recent intrusion into Microsoft's systems appears to have been caused by just such activity[3]. A telecommuting employee's home system apparently became infected with the QAZ trojan which was then transmitted over the virtual private network (VPN) set up between the telecommuting user and Microsoft. The QAZ trojan is a remote execution software that is placed on a computer through an e-mail attachment, usually a Word document. Once the document is opened the underlying macro is executed and sends the hacker a message that it has infected a particular machine. The QAZ trojan then sits waiting on the machine for instructions from the hacker. It is quite likely that the perpetrator of the trojan merely got 'lucky' to be able to get it onto a Microsoft employee's home computer, and then on to the Microsoft system. But how much more could be done if a perpetrator was actually targeting a particular business?

Companies who allow telecommuting should carefully evaluate the methods they will use to allow their employees to connect with the company network. Installation of a personal firewall and up-to-date anti-virus software on the connecting computer could go a long way to protect the company network from the passage of trojans and viruses from the employees location to the corporate network[4]. However, how does a company enforce a requirement that a telecommuting employee place a personal firewall and anti-viral software on the connecting computer if that computer is personally owned by the employee? Should the company dispatch technicians to their employee's homes to install and configure these software packages or should the company allow the employee to install and configure these packages? Obviously the best solution is for the company to provide the telecommuting employee with a company owned computer that is properly configured for connecting to the company network. This adds cost to the telecommuting effort but it can be money well spent to protect the company resources.

E-Mail. Companies may want to include a section that specifically addresses proper use of the e-mail system. Items such as how long e-mail is retained on the company servers, how the e-mail could be used in litigation, and the legal ramifications of agreements made using e-mail should be addressed. In addition the company may wish to include cautions regarding addressing of e-mail to insure the e-mail is properly addressed to the intended recipient. The policy should also inform employees that the company reserves the right to access and monitor all e-mail messages stored on its computer system, regardless of their origin or content.

It may be necessary to caution users about using e-mail to send export controlled or company sensitive data. The company should insure that proper controls are in place to protect the rights of the company and to comply with export control laws.

If the company intends to monitor user's e-mail activity the company may want to include

a prohibition against the use of internet mail systems since mail sent via these systems cannot be monitored. In addition the company may wish to restrict or deny access to anonymous remailers.

Internet Usage. The use of the Internet is probably the area that has caused the most problems for companies. The temptation to stray into non-business related sites can be overwhelming for some people. Businesses should be clear in the acceptable use policy as to what type of Internet activity is considered appropriate. The company may want to consider alerting the employees if the company will be providing supervisors with summaries of their employee's Internet activity. In addition the company may want to define how it will handle the discovery of employees visiting adult sites.

There are a number of threats to the company's data other than specific site content. Companies such as Napster have been set up to provide peer to peer networking for the purpose of sharing files. Companies should consider whether they will allow users on their network to access such sites. In addition these sites can be a threat to the companies telecommuting population if they are accessed using company portable computers which probably contain company sensitive information.

Another threat is the offer of free storage space on the Internet. There are companies that offer users significant amounts of web accessible free storage. The benefit is that it is available from anywhere. The disadvantage is that the company cannot control what data is sent to these sites by their users. Therefore users could be sending huge amounts of the companies data to one of these sites which the employee could then offer for sale to the company's competitors.

If the company will be using systems to block access to particular sites the company should consider alerting the users to that in the acceptable use policy. The company may want to consider a statement indicating a right to block access to any Internet site without prior notice.

Software. The issue of unauthorized software use is looming larger every day in the business place. The Business Software Alliance has become very active in prosecuting businesses found to be using unlicensed software. The company may wish to include a prohibition against users loading software not provided by the company.

1 Shipley, Greg. "How Secure is Your Network?" 27 November 2000 URL: http://www.networkcomputing.com/1123/1123f1.html (20 Nov 00).

2 Mell, Peter. "Computer Attacks: What They Are and How to Defend Against Them". May 1999. URL: http://www.itl.nist.gov/div893/staff/mell/pmhome.html (18 Nov 00)

3 Babcock, Charles. "Experts Ponder the Microsoft Attack." Interactive Week. 9

November 2000. URL: http://www.zdnet.com/enterprise/stories/main/0,10228,2652161,00.html (21 Nov 00)

4 Vaughan-Nichols, Steven. "Taking Security Home Could be Money in the Bank." 20 November 2000. URL: http://www.zdnet.com/enterprise/stories/security/0,12379,2655795,00.html (21 Nov 00)

Last Updated: July 25th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event