Global Information Assurance Certification Paper

IT Security Awareness Best Practices

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4b

Option 1 - Research on Topics
in Information Security

Submitted by: James Neidich
Online Mentor Program
October 8, 2004

IT Security Awareness influences positive behavior and attitude changes of individuals, enhancing the overall security posture of organizations who rely on Information Technology to perform day-to-day operations.

Table of Contents

List of Figures

Abstract/Summary

This IT Security Awareness Best Practices document outlines the processes and procedures in order to conduct a successful and effective awareness training program. It begins by discussing why IT security awareness is important and beneficial to put into practice. The document then goes on to reference relevant federal laws and defines associated IT security terms. The federal laws are then interpreted, providing important topic areas to train that will satisfy the federal requirements.

Section 4 provides sample IT security awareness training materials. These materials include procedures and policies that can be considered best practices. The document goes on to reference additional sources that provide more information not only on IT security awareness, but on IT security best practices as a whole.

1. Introduction

Information Technology (IT) Security Awareness is an issue of concern among many employers, employees, and the everyday IT user. This attention does not come without reason, Denial of Service (DoS) and other malicious attacks cost companies millions of dollars every year. This makes it vital that companies and organizations develop a robust IT security program. IT security awareness is a pivotal and foundational step to any and every IT security program. It is in the best interest of companies everywhere to spend money up front on IT security in order to protect their assets, or it will inevitably cost them more money in the end if they do not. The federal government has passed laws requiring federal IT system and those who operate them to maintain an IT security program consisting of standard policies and procedures.

General IT security awareness has been mandated by law for users of Federal IT systems. The Computer Security Act of 1987 requires each federal agency to "provide for the mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved in the management, use or operation of each federal computer system within or under the supervision of that agency." The law further states that in designating a training program, the objectives should include enhancement of employee awareness of the threats and vulnerabilities of computer systems and the encouragement in the use of improved computer security practices (Public Law 100-235, 1988).

Additionally, the Federal Information Security Management Act (FISMA), as part of the Electronic Government Act of 2002, requires that Federal Departments and Agencies train personnel who have responsibilities for compliance with IT security requirements and related policies, procedures, standards, and guidelines. FISMA requires that IT security awareness programs associate risk levels for personnel and their positions, as well as explain the agencies policies and procedures designed to reduce such risks and how to maintain compliance with them (Public Law 100-347, 2002).

1.1 Purpose

The purpose of IT Security Awareness is to provide personnel with general information meant to promote behavior and attitude changes both at the individual level and at the organizational level. Awareness allows individuals to recognize the importance of security and the consequences that can occur if it is disregarded or ignored. At the individual level, awareness can influence decisions on when providing personal information that may constitute an infringement related to personally identifiable information. At the organizational level, awareness may encourage personnel to challenge an individual's credentials if not openly identifiable.

1.2 Scope

This IT Security Awareness document will benefit both technical and non-technical audiences. The technical individual will gain refresher awareness while non-technical may gain practical awareness, which may influence behavior and attitude changes that will lead to conscientious security practices.

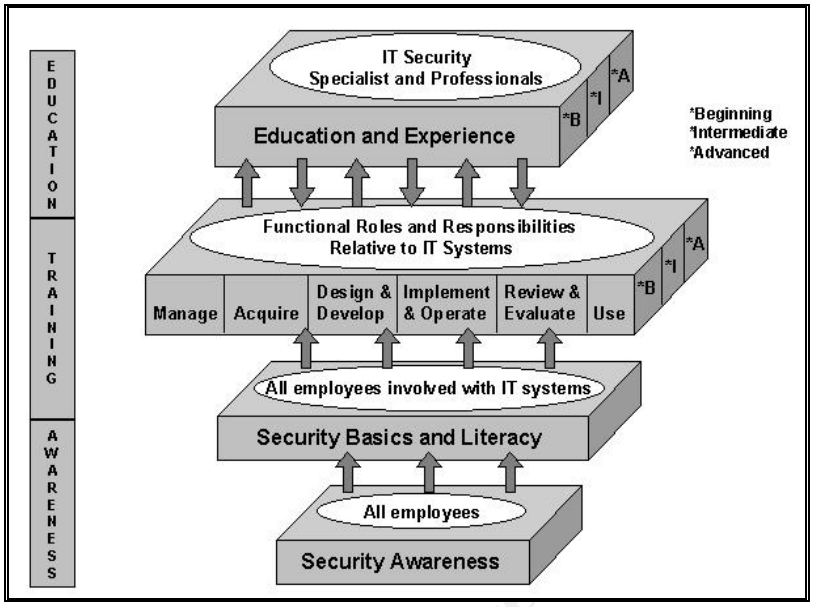
2. Definitions and Goals

According to the National Institute of Standards and Technology (NIST), awareness is meant to focus attention on security. Generally, IT security awareness promotes behavior and attitude changes, both at the individual and organizational level. This is accomplished by developing messages that foster broad-based recognition and retention of general principles. Well-planned and coordinated awareness training can effectively spread understanding of the importance of IT security and encourage security-conscious workforce behavior. It should be noted, however, that while IT security awareness can change individual behavior, it might not directly impact performance of job duties (NIST SP 800-16, 1998).

IT Security is everyone's responsibility, through awareness one will be able to conscientiously protect the confidentiality, integrity, and availability of IT resources, data, and facilities. The term IT resources refer to computers, servers, and networks. Data includes information such as social security numbers, bank account numbers, and passwords. Facilities for our purposes will refer to buildings and rooms that house IT resources and data.

The IT Security Learning Continuum from NIST SP 800-16, shown in Figure 1, represents the instructional best practice for IT Security Awareness, Training, and Education Programs. The model is created from requirements of several Federal regulations to include OMB Circular A-130, Appendix III. Although this figure presents too broad of a scope for our purposes, it does depict IT security awareness as the basis to the rest of a complete IT security training program (p. 13).

Figure 1: NIST 800-16 IT Security Learning Continuum



2.1 Confidentiality

Confidentiality refers to the safeguarding of information against unauthorized access (Information Security Glossary). Security awareness training can inform personnel about practices to ensure confidentiality. Training personnel on topics such as "piggybacking" can help to protect the confidentiality of companies by keeping intruders out. "Piggybacking" is when individuals who do not have proper credentials follow closely and enter directly behind individuals who have access to restricted areas. A suggested practice is to call these individuals out and challenge their credentials (Cole).

2.2 Availability

Availability ensures that the data is accessible upon request to authorized users at a given moment in time. An example of loss of availability is a DoS attack. A DoS attack can be very costly and disrupt business and mission critical functions of companies. IT security awareness training can inform personnel on how to protect the availability of data. Topics to be covered include patch management and the identification of suspicious email attachments (ISG).

2.3 Integrity

Integrity ensures that the data transmitted is true and unchanged. Data integrity is vital when dealing with sensitive data, which can mean the difference between life and death. It is important to maintain data integrity as not to mislead those who view the data. IT awareness training can help to inform personnel on how to watch out for spoofed or altered data (ISG).

2.4 Protecting Resources

The idea of protecting resources is to limit system access to those individuals who are authorized and have a valid purpose for accessing them. This also includes password security. A system is only as secure as the security practiced by the personnel who operate or access it.

2.5 Protecting Data

The idea of protecting data deals primarily with information on both an organizational and a personal level. When protecting data it is important to understand availability, integrity, and confidentiality. Data compromise can lead to data modification or leak company secrets and other proprietary information.

2.6 Protecting Facilities

The idea of protecting resources deals mostly with personnel security. Threats to facilities include intruders, unauthorized personnel, and improper utilization of safeguards. This could be as simple as forgetting to lock a door, failing to follow escort procedures, or by ignoring individuals that appear suspicious, such as strangers hanging around outside entrances and exits. These weaknesses leave security open for the opportunist, who is the easiest to keep out if proper procedures are followed.

3 IT Security Awareness Training

IT security awareness is not innate; it must be promoted in some form of training. There are many different ways to train IT security awareness. Probably one of the most successful and far reaching methods is to develop an online course. An IT security course should be easy to access and navigate by all users.

IT security awareness should follow the standards provided in FISMA Subchapter III, Section 3544. Compliance to FISMA can be achieved by following the interpretations and guidance provided by NIST SP 800-16. NIST is an industry-accepted provider of standards, guidelines, and best practices for the creation of robust IT security programs (CSRC).

FISMA policy states that Individual's activities related to Information Security and Risk should address the following requirements:

- Cite the applicable Policies and Laws associated with security awareness and the importance of compliance and the impact on individual and enterprise IT security.
- Define relevant IT security terms such as threats, vulnerabilities, risk, asset, and impact.

- Discuss assets to be protected and explain the reasons for safeguarding them.
- State the organization's posture and requirements for maintaining confidentiality, integrity, and availability
- Describe various types of threats and vulnerabilities and how to recognize when and where security problems exist.

In addition to citing policies and laws, a robust IT security awareness program should address the rules of behavior, as well as describe roles and responsibilities for complying with policies and procedures (Public Law 107-347, 2002).

The rules of behavior should state the company's policies regarding email, web browsing, passwords, and various others. The rules of behavior should be read and signed by all staff (Public Law 107-347, 2002).

The roles and responsibilities should identify the importance of each individual user's role as it relates to IT security. It should also stress how important it is that each individual understands what their role is and how to perform it effectively (Public Law 107-347, 2002).

One of the best methods to promote IT security is to use entertaining and fun activities such as games, movies, and books. Listed below are some examples:

- Security Crossword Puzzles
- Security Awareness Day
- Show a Movie (e.g. Sneakers)
- Promote reading (e.g. The Cuckoos Egg, by Cliff Stoll)

4. Sample IT Security Awareness Products

Awareness is a learning process that changes organizational behaviors as well as attitudes and perception. This is done in an effort that allows personnel to realize the importance of security and the consequences of failure to adhere to security policies and procedures. Awareness can include a variety of products used to identify specific security messages and target them to a broad audience. Listed below are examples awareness products.

4.1 Security Tip of the Week

The Security Tip of the Week will assist in heightening employees' security knowledge and awareness for securing and safeguarding IT systems, facilities, and personnel. The Security Tip of the Week can be distributed via email to

personnel, as well as be available online. A Security Tip program has the capability to reach all employees and support management's goal of making security a number one priority.

4.1.1 Desktop Checklist

There are several daily steps that the one should follow to protect the information that is stored, processed, and transmitted on IT systems. The following presents a desktop checklist, drafted from guidance provided in NIST SP 800-26 that can be used to test yourself on whether you are following proper IT security procedures.

- Do not write down or share your password
- Password protect your screensaver to prevent others from using your system while you are away
- If you deal with sensitive information, use only pre-approved computers, copiers, and fax machines.
- Make sure that you secure any sensitive data in your office by locking it away.
- Protect removable media (e.g. diskettes and CD-ROMS) and portable computer resources such as laptops from loss or theft
- Only install authorized software to your computer
- Backup your hard drives on a regular basis
- If you are provided with server storage space, make use of it and store data on it rather than your hard drive.
- Log off and shut down your computer at the end of the day
- Make sure to lock away sensitive information at the end of the day, also if possible, lock your office door (NIST SP 800-26).

If you have any questions or concerns related to IT security, contact your security officer.

4.1.2 What is Security?

Security is everyone's job. Know your security responsibilities.

All employees have an obligation to protect and safeguard facilities, operations, information, systems, and personnel. Security is not "someone else's job." What are some of your responsibilities? These responsibilities are drafted from guidance provided in NIST SP 800-26, "Security Self-Assessment Guide for Information Technology Systems."

Select a strong and secure password for access to systems. Strong and secure passwords consist of at least 8 characters with a combination of upper and lowercase letters, numbers and special characters. (e.g., 4H@cker$2Net)

Escorts must accompany individuals who are not authorized and approved for access within certain Facilities.

Computers, such as Laptops, that leave facilities shall maintain updated virus definitions and be scanned for viruses before they are connected back to networks.

Use only approved software, computers, and communication devices for processing, storing, and transmitting material.

Report all incidents and events in violation of policies and procedures to the appropriate Security Officer.

Insist that personnel do not use their personal computers to process, access, and store sensitive information without the approval of management.

Terminals, workstations, and networked computers should be locked whenever unattended, especially while logged in.

You must use discretion when discussing sensitive information outside of company space, be aware that others around you, may be eavesdropping.

Know your security responsibilities. Think secure, and be secure!

4.1.3 Password Security

Passwords are the means used to authenticate an authorized individual to an information system. In many instances passwords are the last line of defense for an information system. If passwords are compromised allowing an unauthorized person to access information the company's mission may falter.

Password compromises lead to the unauthorized access and potential damage to official files; compromise of databases; an inability for legitimate information system users to access information they need to do their jobs; sensitive information could be unknowingly altered; and information could be accessible to individuals without a valid "need-to-know" (NIST SP 800-12).

For these reasons and others, all users of information systems must ensure that their passwords meet the following requirements, which were derived from guidance provided by NIST SP 800-12:

1. Passwords must contain at least 8 characters and be a combination of uppercase and lowercase letters, numbers, and special characters. Passwords should not resemble any word, name, idea, or concept that can be found in the dictionary or can be easily associated with the individual, such as their last name or the name of their favorite sports team.

2. Do not write your passwords down and stick them on your monitor. If you must write your passwords down, store them under lock and key. Passwords are one of the last lines of defense to keep out unauthorized individuals.

3. If a password is compromised it should be reported at once to your system administrator and security officer. System administrators should immediately remove privileges to compromised passwords.

4. Do not allow others to use your password. Passwords should not be shared; each user should have their own unique password.

5. Do not log into your workstation while other are watching. Also be courteous to others and look away while they are logging into their system.

4.2 On-line Training

On-line training is an effective method to reach a broad based audience. Here are some sites that offer free IT security awareness training:

- Gov Online Learning Center provides a variety of online training courses for government employees.

- The National Institute of Standards and Technology (NIST) offers additional Training Events.

4.2.1 Security Threat Information

Visit Symantec to view the most recent security threats. Symantec offers detailed information on viruses and worms. They also offer patches to fix the problems associated with the latest security threats (Symantec).

Check out these related sites:

- www.sophos.com

- www.networkassociates.com
- www.cert.org

4.2.2 Policy and Law

Visit the Computer Security Resource Center to read up on mandated federal IT Security policies and laws, as well as industry accepted best practices for implementing IT Security:

- Policy and Laws, available online at: http://csrc.nist.gov/policies/
- Best Practices, available online at: http://csrc.nist.gov/publications/nistpubs/index.html

5. Conclusion

The best practices set forth in this IT security awareness document assist in the development of curriculum to compliment a Security Training and Awareness Program. Through a well-designed and executed Security Training and Awareness Program, an organization will be better prepared and poised to protect the confidentiality, integrity, and availability of their information and information resources.

References

Cole, E. (December 2003). “Physical Security.” SANS GIAC Security Essentials Boot Camp. (Archived Audio File).

Computer Security Resource Center (CSRS) National Institute of Standards Technology (NIST). “Information Technology Laboratory.” Retrieved October 7, 2004, from < http://csrc.nist.gov/>.

CSRS NIST. “Events.” Available Online at: <http://csrc.ncsl.nist.gov/events/index.html>

The Information Security Glossary (*ISG*). (n.d.). Retrieved September 29, 2004, from <http://www.yourwindow.to/information-security/gl_confidentialityintegrityandavailabili.htm>.

National Institute of Standards Technology (NIST) Special Publications (SP) 800-12. *An Introduction to Computer Security. The NIST Handbook*, October 1995. Available Online at: <http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/index.html>

NIST SP 800-16 *Information Technology Security Training Requirements: A Role- and Performance- Based Model*, April 1998. Available Online at: <http://csrc.nist.gov/publications/nistpubs/index.html>

NIST SP 800-26 *Security Self-Assessment Guide for Information Technology Systems,* November 2001. Available Online at: <http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.doc>

Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, November 28, 2000.

Office of Personnel Management (OPM). “Gov Online Learning Center.” <http://www.golearn.gov/>

Public Law 100-235 [H.R. 145], *The Computer Security Act of 1987*, January 8, 1988. Available Online at: <http://cio.doe.gov/Documents/CSA.HTM>

Public Law 107-347 [H.R. 2458], *The E-Government Act of 2002 Title III of this Act is the Federal Information Security Management Act (FISMA)*, December 17, 2002. Available Online at: <http://csrc.nist.gov/policies/FISMA-final.pdf>

Symantec. “Global Security Solutions” Available Online at: <http://www.symantec.com/index.htm>