Global Information Assurance Certification Paper

Patty Hisey

Computer Security Awareness Training…Do you need it?

In March 2000, the Computer Security Institute/FBI Computer Crime and Security Survey revealed that 90% of respondents detected some sort of computer breach within the last 12 months. The quantified financial losses of respondents were $265,589,940.00. Would you expect one person to be able to prevent this kind of loss? Can you afford not to have Security Awareness all the way down to the user level?

Computer Security is defined, as the safeguard controls required to protect an IT system based on identified needs for confidentiality, integrity and/or availability. **Awareness** is a learning process that sets the stage for training by changing individual and organizational attitudes. So **Computer Security Awareness** would be the process of learning the safeguard controls used or needed to protect the IT system based on the need for confidentiality, integrity and/or availability.

A good computer security awareness program will educate your employees' to the potential threats levied against your company's infrastructure. With this knowledge employees' should be empowered to recognize a potential security problem. Once the problem has been identified the employee should know the proper reporting procedure. The program should be able to change employees' perception of security from something that is a burden to a necessity. This program cannot be a one-time event. Security threats and vulnerabilities are ever changing. Security needs to become a habit not an exception. Presentation of the program can be in any form. A creative combination of the below is the best way of presentation.

Posters
Newsletters
Mouse Pads
Pamphlets
Stress Balls
Screen Saver
E-Mails
Daily messages
Pens

The benefits to providing a good, well-constructed security awareness programs are numerous. To raise the level of awareness within your organization for the need of security, people must see the problem. Publicizing your security policy, showing why it is needed and identifying areas that need improvement will help your people become aware of how important security is and the vital role they play. With employee cooperation and buy-in to your security policy you reduce your liability. Less system outage and/or downtime means you save money and time. Employees who understand

security measures and why we need them give management more support to new changes.

The topics that you can use for your awareness program are numerous and can relate only to your company. It is best not to present all the topics at one time. Breaking them down into several short session or messages will not only save time and resources but keep employee attention. Remember the key is for employees to learn about security not just to meet some requirement. Here is on outline of possible topics to address. This is not an all-inclusive list but suggestions.

A. Internet Security
    1. Attackers, Hackers and Crackers
        a. What is an Attack / Attacker
        b. What is a Hacker
        c. What is a Cracker
        d. What is are Script Kiddies
    2. Internet Vulnerabilities
        a. Increased Usage
        b. Always-on Connections
        c. Insure Technology
        d. Lack of Education
    3. Ways of Hacking into a system
        a. Port Scanning
        b. Denial of Service Attacks
        c. Viruses
        d. Malicious Code
        e. Trojan Horses
        f. Worms
    4. Losses from attacks or hacks
        a. Loss of Information
        b. Data theft
        c. Launching Attacks from you system

B. Passwords
    1. General Rules for passwords
        a. Don't Share
        b. Never Write down
        c. Don't store on your computer
        d. You type in your password, not the technical support person
        e. If you receive a phone call and the person requests your password, report it immediately
    2. Strong Passwords
        a. No familiar names
        b. Avoid commonly known facts about yourself
        c. No dictionary words

d. At least 8 characters
e. Use uppercase and lowercase letters, numbers and special characters
f. Combine mis-spelled words
g. Use 'Vanity' passwords {just like 'vanity' plates for your car}
h. Use Passphrases
i. Create Keyboard Pattern passwords

C. Physical Security
1. Know who is in your area
2. Know who is trying to use your computer
3. Lockup sensitive data

D. E-mail
1. You can control what you send out
2. Don't send sexually explicit, racist or other offensive material
3. Follow the company rules and regulations closely
4. Disciplinary actions can happen for misuse of email

E. Laptops
1. Keep laptop clean of sensitive data
2. Try encryption for laptops with sensitive data
3. Don't leave unattended
4. Don't open unknown email attachments
5. Install anti-virus software

F. Securing your Home PC
1. Install anti-virus protection
2. If not connected to other PCs, disable "Client for Microsoft Networks"
3. If not connected to other PCs, disable "File and Print Sharing"
4. Use dial-up connection for access to internet
5. Set administrator password
6. Install a personal firewall
7. Strong passwords and periodically change them

G. Social Engineering
1. What is Social Engineering
2. How to prevent it

H. Chats
1. How they work
2. Realize it is realtime

I. Security techniques
1. Locking your terminal before you leave the area
2. Creating strong passwords

3. Backups

J. Palm Pilots / PDA
   1. Install anti-virus software
   2. Same precautions as regular computer
   3. Limit sensitive data
   4. Don't store passwords

K. Disaster Recovery
   1. Have a plan
   2. Publish your plan so employees are informed
   3. Test your plan

L. Cryptography
   1. What it is
   2. How it works

M. Incident Reporting
   1. What is an incident
   2. When to report
   3. Who to report to

If you still do not see the need for a Computer Awareness Program read these 10 Laws cited from Microsoft Technet. If you think your company does not need a small army of well informed employees then your computer will probably not be yours for long.

The Ten Immutable Laws of Security

Law #1	If a bad guy can persuade you to run his program on your computer, it's not your computer anymore.
Law #2	If a bad guy can alter the operating system on your computer, it's not your computer anymore.
Law #3	If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.
Law #4	If you allow a bad guy to upload programs to your web site, it's not your web site any more.
Law #5	Weak passwords trump strong security
Law #6	A machine is only as secure as the administrator is trustworthy.
Law #7	Encrypted data is only as secure as the decryption key.
Law #8	An out of date virus scanner is only marginally better than no virus scanner at all
Law #9	Absolute anonymity isn't practical, in real life or on the web.
Law #10	Technology is not a panacea.

Computer Security Institute. "Percent of Organizations Reporting Internet Attacks." URL: http://nativeintelligence.com/percent-no.asp (Nov 29, 2000).

National Institute of Standards and Technology. "Glossary of Terms Used in Security and Intrusion Detection." URL: http://patapsco.nist.gov/itl/div893/gits/glossary.htm (Nov 29, 2000).

Jenkins, Joe. "Internet Security and Your Business – Knowing the Risks." Nov 6, 2000. URL: http://www.securityfocus.com/focus/basics/articles/risks.html (Nov 29, 2000)

Security Awareness. "Password Management." URL: http://www.securityawareness.com/managepw.htm (Nov 29, 2000)

Native Intelligence. "Can an employee be fired because of an e-mail?" URL: http://nativeintelligence.com/fired.asp (Nov 29, 2000) and "Internet Security" URL: http://nativeintelligence.com/internet.asp (Nov 29, 2000)

Microsoft Technet. Culp, Scott. "The Ten Immutable Laws of Security." Oct 2000. URL: http://www.microsoft.com/technet/security/10imlaws.asp (Nov 29, 2000)

Ascii Technology Inc. "Security Awareness Training." URL: http://www.asciitech.com/Services/Security/Products/sec_SAT.html (Nov 29, 2000)

© SANS Institute 2000 - 2005 Author retains full rights.