Global Information Assurance Certification Paper

IMPLEMENTING A SECURITY AWARENESS TRAINING PROGRAM IN YOUR ENVIRONMENT FOR EVERY DAY COMPUTER USERS.

Kelly Nichol
December 18, 2000

"Security is a chain; it's only as secure as the weakest link."
-Bruce Schneier Secrets & Lies Digital Security in a Networked World c. 2000

INTRODUCTION

All it takes is just ONE weak link in the chain for an attacker to gain a foothold into your network. Because human beings are usually considered to be the weakest link in the security chain, implementing a security awareness-training program for your computer users is a must. A company's information system can not be secured properly unless the computer users have been properly trained in security awareness according to their job functions. "The statement that 'security is everyone's responsibility' is absolutely true." [2]

What exactly does security awareness training mean? Based on the definition from National Institute of Standards and Technology:

Awareness, Training And Education Controls	include (1) awareness programs which set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure, (2) training which teaches people the skills that will enable them to perform their jobs more effectively, and (3) education which is targeted for IT security professionals and focuses on developing the ability and vision to perform complex, multi-disciplinary activities. [3]

IMPLEMENTATION

Our organization has successfully implemented a security awareness-training program for our computer users for the last two years using internal resources. Our organization has several methods of computer

security awareness training we have found helpful and the best part is that the costs associated for implementations are mostly time related.

One method is a 15-minute presentation at the monthly New Employee Orientation meetings. The employees each receive a handout to go along with the presentation. Included in the handout is an outline of the presentation, our security policy summary of "general user" topics, and two security posters, one on "strong passwords" and one with good security practices that users can go back and reference after the presentation.

Following is an example of the outline our organization uses for our security presentation. Extra time is spent going over how to create strong passwords, as passwords are an area on which an attacker will focus attention.

- **Who we are?**
- **What are our responsibilities?**
  Responsible for the security of all computing systems in our environment
  Provide ID's to access computing environments
  Provide Data access
  Provide security policies, procedures, standards and guidelines on information systems security
  Provide information and assistance to users and system developers.
- **What are your responsibilities?**
  Security Policy – know what it says (reference security policy handout)
  Use strong passwords (reference poster included in handout)
  Keep your password confidential
  Use assigned computers, software, and Internet access for business only
  Use email for business purposes only – personal emails are not permitted
  Copying software is illegal
  Lock workstation
  Be aware of Social Engineering
  Protect the data that you "own"
  Review access permissions regularly on data that you "own"
  Store data on a server (not your C: drive)
  Read bi-monthly security awareness articles in newsletter
  Diskettes scanned for viruses

Contact Security Unit for unexplained password resets, general advice and counsel

Another method our organization uses for security awareness training is a bi-monthly newsletter that our Information Systems Branch publishes in which the security unit has a "Secure Computer Corner" for articles related to this subject. Some topics we have included are strong passwords (we try to bring this to users attention regularly); data security; security related posters, and a "test your security knowledge" quiz (which we found to be one of our most successful articles).

Our unit was pleasantly surprised at the response and feedback generated by our quiz, 99% of it very positive. Employees who answered the questions correctly received a certificate suitable for framing, which recognized their demonstration of accurate knowledge of our organization's Computer Security Awareness practices. The results of the test were very helpful for our unit in deciding where we need to focus our training efforts.

The third method we have for training is a 28-minute training video "Responsible Computing: It Is A Big Deal!" We obtained this video from Southwestern Bell Telephone. With the video comes a Leadership Guide[4] which has suggestions on how to present the video and how to elicit audience participation which we have found very helpful. We show this video at our quarterly New Manager Orientation Meeting and have found the managers find it entertaining as well as informative. We feel showing it to managers is good for their own security awareness training and enables them to assist their employees in maintaining good security practices. We also offer to come to their team meetings with their employees to show the video and do a short security presentation. This way we reach employees that may not have attended the new employee orientations.

One source for security awareness training videos is from Commonwealth Films. "With a library of nearly 80 videos, Commonwealth helps organizations educate their employees about today's top business issues including: legal compliance in areas such as antitrust, environmental issues, and sexual harassment; computer security, information protection, e-mail misuse, and Internet abuse." [5]

The company includes brief topic outlines of the various security awareness-training videos, the length of the video, the cost and any training materials that you can purchase to go along with the videos.

While searching the Internet you can find various resources for topics for your security awareness training. One of the helpful ones I've come across are the Computer User's Guide to the Protection of Information Resources [2] which has basic understandable guidelines for Federal computer users, which translate very well to state governments and/or the private sector.

CONCLUSION:

Computer Security depends on all of us, not just the technical employees who setup and monitor the organizations network, the traditional area people tend to focus regarding security. Every organization should have some sort of computer security awareness training for their employees. The security of your computer networks depends on it.

REFERENCES:

1. Bruce Schneier, Secrets & Lies Digital Security in a Networked World, c. 2000

2. Helsing, Cheryl. Swanson, Marianne. Todd, Mary Anne. Computer User's Guide to the Protection of Information Resources. URL: http://nsi.org/Library/Compsec/usergide.txt

3. Federal Computer Security Program Managers Forum and the Federal Information Systems Security Educators' Association (FISSEA) "NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model." April 1998, URL: http://patapsco.nist.gov/itl/div893/gits/glossary.htm

4. Grindler, Jacqueline M. Leadership Guide "Responsible Computing Only YOU Can Make It Happen!" 1996

5. Commonwealth Films Inc. URL: www.commonwealthfilms.com/infosec.htm