Global Information Assurance Certification Paper

Chi Kim Hoang
GSEC Practical Assignment version 1.4b

Employees are your security

Introduction:

"An educated and aware user is the foundation of a secure and reliable computing environment." Ask any end user in your company if the security of the corporate network, systems and data is in any way their responsibility and you are likely to get the common answer, " No, the IT guys take care of that." In reality, all of your employees have a responsibility toward Information Security and a role to play in reducing the risks your business is exposed to on a daily basic. By increasing the security awareness of end users, your organization can make tremendous strides in increasing the overall security of its information infrastructure.

What is Security Awareness?

Security Awareness means understanding the **various threats** that exist in one's environment and taking reasonable steps to guard against them. Security awareness also clearly defines the proper, safe and secure use of that very powerful tool, the Internet, for which most, if not all, users are connected.

The Important of Security Awareness

Many organizations spend a significant amount of time and money addressing the technical aspects of information security while spending only a comparative fraction on addressing the human aspects of security. This imbalance is often counterproductive: in securing technologies and then relying on technology for security, organizations leave themselves exposed to human vulnerabilities. Remember that information systems include information, technology *and* people.

Bruce Schneier, a computer security expert and CEO of Counterpane Internet Security, Inc, once said, "Amateurs hack systems, professionals hack people". The most effective attacks on information are social engineered attacks.

The need for employee involvement in information security is clear. Ninety percent of large corporations and government agencies detected computer security breaches in the United States in 2001, according to the 2002 Computer Security Institute/FBI Computer Crime and Security Survey. Eighty percent of those organizations acknowledged financial losses due to security breaches. In an effort to better protect themselves from such losses, many organizations have implemented robust, integrated security systems, yet they often fail to plug a

major security hole — employees. However, with proper planning and training, what was once a security weakness can quickly become a strong defense.

Education can't be effective and concise if the material is too complex. That is why well-crafted security policies are so important. The source material needs to be distilled into digestible components.

An education program should consist of:

- **Initial training:** New employees should receive baseline instruction on policies, issues and response/reporting. Training should be pertinent to their job within the enterprise and be short enough to keep their attention. It can range from classroom to computer-driven self-study modules. At the end of sessions, new employees should be quizzed briefly on essential elements and sign a statement that they understand the content.

- **Periodic training:** The essential elements from the initial training should be reviewed, as well as updates to policies and procedures. Employees should be re-quizzed on content and sign a new agreement. Depending on the nature of your business, training can be performed annually, quarterly or as needed.

- **Ongoing programs:** On going programs are on of the most effective tools of the security-aware enterprise. They include traditional methods such as wall posters, handouts and memos, as well as more interactive methods such as monthly e-mail updates, intranet-based Web games, and special bulletins concerning internal and external security incidents. Ongoing training can take advantage of media events like Code Red and the Loveletter virus by showing employees the material impact.

- **Ongoing assessment:** This will vary highly depending on the resources of the enterprise and their actual security needs, but appropriate and random assessments should be performed to ensure training is effective. Consider ongoing assessment as the "fire drills" of corporate security.

- **Quality assurance on training and trainers:** It's important to get feedback on the training programs, material and trainers themselves. Those responsible for training should include quality assessments as part or the program.

The following section contains information about the various security threats that is necessary for employees to understand in order to guard against them.

Security Threats:

Threats can originate from two primary sources: humans and nature. Human threats subsequently can be broken into two categories: malicious and non-malicious. The non-malicious "attacks" usually come from users and employees who are not trained on computers or are not aware of various computer security threats. Malicious attacks usually come from non-employees or disgruntled employees who have a specific goal or objective to achieve.

Natural Disasters

Earthquakes, hurricanes, floods, lightning, and fire can cause severe damage to computer systems. Information can be lost, downtime or loss of productivity can occur, and damage to hardware and other essential services can be disrupted.

Few safeguards can be implemented against natural disasters. The best course of action is to have disaster-recovery and contingency plans in place. These will help an organization restore itself to normal business operations.

Insiders or Malicious and Disgruntled Employees

Insiders are likely to have specific goals and objectives, and have legitimate access to the system. Employees are the group most familiar with their employer's computers and applications, including knowing what actions might cause the most damage. Insiders can plants viruses, Trojan horses, or worms, or browse through the file system. This type of attack can be extremely difficult to detect or protect against.

The insider attack can affect all components of computer security. By browsing through a system, an insider can learn confidential information. Trojan horses are a threat to both the integrity and confidentiality of information in the system. Insiders can affect availability by overloading the system's processing or storage capacity, or by causing the system to crash.

These attacks are possible for a variety of reasons. On many systems, the access control settings for security-relevant objects do not reflect the organization's security policy. This allows the insider to browse through sensitive data or plant a virus or Trojan horse. Often these actions are undetected because audit trails are inadequate or ignored.

Disgruntled employees can create both mischief and sabotage on a computer system. Organizational downsizing in both public and private sectors has created

a group of individuals with organizational knowledge who may retain potential system access. System managers can limit this threat by invalidating passwords and deleting system accounts in a timely manner. However, disgruntled current employees actually cause more damage than former employees. Common examples of computer-related employee sabotage include:

- Changing data
- Deleting data
- Destroying data or programs with logic bombs
- Crashing systems
- Holding data hostage
- Destroying hardware or facilities
- Entering data incorrectly

Recently, a former Viewsonic employee who was terminated early last year working as a network administrator was arrested, he deleted some critical files on system that he maintained crippling that server for several days since others could not access this important data. For more detail, please visit this link: http://www.ebnonline.com/showArticle.jhtml;jsessionid=GY15MZRQTAPZKQSNDBGCKH0CJUMEKJVN?articleID=6511957

Another example, From ITWorld.com (published on 26 Nov 02), an identity thief ring was uncovered by federal investigators. Philip Cummings, while working at Teledata Communications Inc., which provide credit report to banks and other entities, uses TCI 's customer password and codes to obtain credit report to sell them roughly at $30 per credit report to others to make purchases with new credit cards with information obtained from these credit reports. He has been selling these credit reports for the past 3 years. As many as 15,000 credit reports from Ford Motor Credit Corp. were illegally obtained.
http://www.itworld.com/Sec/3495/021126identity/

Outside Attackers or 'Crackers'

People often refer to "crackers" as "hackers." The definition of "hacker" has changed over the years. A hacker was once thought of as any individual who enjoyed getting the most out of the system he or she was using. A hacker would use a system extensively and study the system until he or she became proficient in all its nuances.

Now, however, the term hacker refers to people who either break into systems for which they have no authorization or intentionally overstep their bounds on systems for which they do not have legitimate access.

The correct term for someone who breaks into systems is a “cracker.” Common methods for gaining access to a system include password cracking, exploiting known security weaknesses, network spoofing, and social engineering.

Attacks to companies that handles credit card transaction frequently made headlines. AP stories on February 19, 2003: Data Processors International ‘s computer system was accessed from “an unauthorized outside party” as much as 8 million account numbers were accessed according to credit card companies and the Secret Service.
From Internetnews.com January 9, 2000: an 18-year-old Russian cracker published on a website with about 25000 stolen card number from CDuniverse.com that use a popular credit card authentication, ICVerify, from CyberCash, after failing to get 100,000 for him to keep quiet about this security breach. These typical stories are just the tip of the iceberg as many untold, undetected or insignificant unauthorized system access on the Internet.

Non-Malicious Employees

Attackers are not the only ones who can harm an organization. The primary threat to data integrity comes from authorized users who are not aware of the actions they are performing. Errors and omissions can lose, damage, or alter valuable data.

Users, data entry clerks, system operators, and programmers frequently make unintentional errors that contribute to security problems, directly and indirectly. Sometimes the error is the threat, such as a data entry error or a programming error that crashes a system. In other cases, errors create vulnerabilities. Errors can occur in all phases of the system life cycle.

Programming and development errors, often called “bugs,” range in severity from irritating to catastrophic. Improved software quality has reduced but not eliminated this threat. Installation and maintenance errors also cause security problems.

Errors and omissions are important threats t data integrity. Errors are caused not only by data entry clerks processing hundreds of transactions per day, but also by all users who create and edit data. Many programs, especially those designed by users for personal computers, lack quality –control measures. However, even the most sophisticated programs cannot detect all types of input errors or omissions.

People often assume that the information they receive from a computer system is more accurate than it really is. Many organizations address errors and omissions in their computer security, software quality, and data quality programs.

Consider some of the most common security mistakes made by your employees

1. **Writing passwords on Post-It-Notes**
   Those sticky yellow notes can undo the most elaborate security measures. Worried that they'll forget their passwords, people stick them to the front of their monitor for the entire world to see.

2. **Leaving computer on without protection**
   Dan Bent, CIO at Benefits Systems Inc., in Indianapolis, says he's amazed at the number of users who leave their machines on and walk away, sometimes for hours. This way, a potential hacker doesn't even need your password

3. **Opening unexpected e-mail attachments**
   "Users open all their e-mail attachments before thinking," says Marie Phillips, manager of information security services at Amerisure Mutual Insurance Cos. in Farmington Hills, Mich. Worms and viruses such as the Love Bug, which can potentially cripple a company's computer systems, spread like wildfire for exactly this reason.

4. **Selecting weak passwords**
   If your password is your birth date, your spouse's name, or other information easily accessible to others, you should pick a new one. In a recent demonstration, anti-hacking experts from NASA took only 30 minutes to break 60% of a group of engineers' passwords

5. **Leaving laptops physically insecure**
   Everyone knows how common it is for laptops to be stolen in public places, but Jay Ehrenreich, senior manager at PricewaterhouseCoopers in New York, says it's surprisingly common for a person to leave his laptop in his office unsecured, unattended, and in full view of passersby. "These things walk," he warns. When you leave the office, you should lock away your laptop.

Education is a critical element of security awareness. It’s hard to be aware of security incidents if you don’t even know what the issues are. Employees need to be trained in the following areas:

- **Corporate policies:** They need to understand policies to both limit their personal violations and allow them to recognize when others violate policies.

- **Security issues:** What is a virus anyway? Employees need training on a variety of security issues, from physical access, to information misuse to

e-mail safety. Ongoing training should include new security issues as they arise, and signs of an impending incident before it causes damage.

- **Impact on the enterprise/employee:** People tend to pay less attention to issues that don't directly affect them. Awareness and proactive actions are more likely if employees understand the negative consequences on the enterprise and themselves.

- **How to report/respond:** Obviously not everyone needs to be trained to put out a fire, but they do need to know how to hit the fire alarm, call 911 and safely evacuate the building.

Security Tips for End User

- **User strong passwords**

  A password is your key for accessing the computerized systems that contain proprietary information. And like any key, it can be stolen. Remember, the person who steals your password steals you identity. The thief who tampers with information using your password is acting with impunity. All the evidence will point to you. Choose your password carefully, and guard it as you would the key to your own home.

  A good password should:

  - Have at least eight (8) characters
  - Contain a mixture of uppercase and lowercase letters
  - Be alphanumeric (contain both letters and numbers)
  - Contain punctuation keys-the used of punctuation keys is critical and can mean the difference between a password that can be cracked and one that cannot
  - Be changed frequently
  - Never be shared, written down, or e-mailed to others
  - Be easy to remember (for you, not others!)

- **Install the latest version of anti-virus software**

  Computer viruses are deadly. Carried on floppy disks, CD ROMs, and e-mail, they can infect your computer and wipe out all information processes instantly. Don't inject deadly viruses into your system. Follow these steps:

- Make sure that virus protection software is installed and running.
- Scan all media such as floppies and CD ROMs, and all electronic documents such as e-mail attachments. This includes media and documents from home computers, business partners, product venders, training agencies, and service technicians.
- Scan all floppies before distributing them to others.
- When you suspect the presence of a virus, report it to your supervisor and the IT Help Desk immediately.

- **Back up your data**
  - Don't store sensitive information on our hard drive unless it is protected by physical, electronic, or administrative-access controls. And don't store information solely on your hard drive. Back up any files that you are responsible for managing. This will protect the information in case you accidentally delete it; the computer crashes, or the software fails also a good idea to periodically test your system's recovery programs and procedures.
  - Both your computer and your removable media can be destroyed by fire, water, or other means. It is wiser to store your backup copies--once they are properly labeled—in a location outside your workstation. Local Data Centers provide off-site storage that is good insurance against destruction.
  - Storing your data files on network drives is the safest choice. IT personnel routinely back up network drives.

- **Protect your account**
  - When logging on, check the "last log-in" message displayed on your screen. Were you the last person to log on as you? Report any irregularity at once to your immediate supervisor and the IT Help Desk.
  - Once you are logged on, your computer screen is open for the entire world to see. Watch out for strangers in your work area. Even a stranger within your organization may be one those shoulder surfers.
  - If you have to leave your workstation during an active session, use your password to lock out. Without screen saver, your computer is

an open book. Remember to turn off your computer before going home or away on a business trip. When there is a valid reason to leave it on, apply your password-based screen saver.

- **Beware of Social Engineering**

  Social engineering is a process of deception through various techniques to obtain critical information that can be used to attack computer systems. In some cases, social engineering techniques are used to induce a person to reveal confidential information.

  Techniques that can be used on you to gather information include:

  - Waste paper basket diving
  - Impersonation of real or fictitious characters
  - Lies and exaggeration
  - Praise of flattery
  - Using authority as a threat
  - Sexual enticement
  - Planting backdoors in programs and Trojan horses as benign applications

  Tips on social engineering:

  - Never give your password to anyone for any reason
  - Verify the identity of all callers
  - Don't give out information about other employees (names, positions, etc.)
  - Never type things into the computer when someone tells you to unless you know exactly what the results of the commands are!
  - Don't give out the dial-in phone numbers to any computer system unless they are valid users
  - Never answer questions from telephone surveys. Tell the caller that employees do not participate in telephone surveys from vendors. If they need information.

Emails

Email can be used to propagate viruses and hoaxes.

If you do not know the person who is sending you an email, be very careful about opening it and any file attached to it. Should you receive a suspicious email, delete the entire message, including any attachment.

Even if you do know the person sending you the email, you should exercise caution if the message is strange and unexpected, particularly if it contains unusual hyperlinks. Your friend may have accidentally sent you a virus. Such was the case with the "I Love You" virus that spread to millions of people in 2001. When in doubt, delete!

Protect outgoing messages. Unprotected e-mail is an open letter to the world. Here are some tips:

- Don't send sensitive information through the Internet.
- Never disclose your e-mail password to another person.
- Do not send information that may breach Company policy or government regulations, including language that could be interpreted as harassing or offensive.

Exercise caution when using the Internet

It is impossible to use public networks and be 100 percent safe. The Internet and other public networks such as America Online and CompuServe are outside the Organization control. The plain-text message sent through such services is as exposed as a postcard. Protect your organization's value trade secrets from a web of thieves; don't announce confidential business on the Internet.

When surfing the Web, be careful with "executable content" such as Java, Jscript, VBScript, and Active X controls. They may contain material that can compromise security.

Conclusion:

I truly believe that without a good and sound employee awareness training, where every employee is taught the ways that they can help with the overall security of their company, most other more expensive countermeasures will be much less effective.

REFERENCES:

1. Matt Loney. “Your worst security threat: Employees?” 4/23/2002
URL: http://zdnet.com.com/2100-1105-889542.html

2. Fenella Quinn, Industry Reporter. “Security survey reveals alarming results”. 2/13/2002
URL: http://humanfirewall.org/articles.asp

3. Rhonda Tamulonis. “Continuous Employee Training.”
http://www.iisw.cerias.purdue.edu/business_industry/continuous_employee_training.php

4. SANS Institute. 10/23/01. “Mistakes People Make that Lead to Security Breaches.”
URL: http://www.sans.org/resources/mistakes.php#top

5. Security Threats.
http://www.windowsitlibrary.com/Content/121/06/1.html#1

6. “The Insider Threat To Information Systems”
URL: http://www.dss.mil/training/csg/security/Treason/Infosys.htm#infosys

7. Top Ten Security Tips For End Users:
http://www.ida.gov.sg/Website/IDAContent.nsf/vSubCat/For+the+ConsumerInfocomm+Security+-+It's+Everyone's+Responsibility?OpenDocument

8. Password Tips
URL: http://www.tufts.edu/tccs/r-strongpass.html

9. K Rudolph, CISSP, Louis Numkin and Gale Warshawsky. “ Security Awareness”
URL: http://nativeintelligence.com/awareness/chap29-2.asp#29.2.3

10. Man charged with crashing employer's computer site.
By The Casper Star-Tribune. February 17, 2003
URL: http://www.securityunit.com/news/

11. Laurie Sullivan. “Former Viewsonic Employee hit with hacking charge” 02/06/2003
http://www.ebnonline.com/showArticle.jhtml;jsessionid=GY15MZRQTAPZKQSNDBGCKH0CJUMEKJVN?articleID=6511957

12. Matt Berger, IDG Ness Service, San Francisco Bureau.
"Feds crack huge identity theft ring". 11/26/02
URL: http://www.itworld.com/Sec/3495/021126identity/