INTRODUCTION
This article focuses on the first step of providing computer and information system security — developing and implementing an effective security awareness program. One might wonder why security awareness is not considered the same as training. The simple answer: because the desired outcome of each is different. The goal of a security awareness program is to heighten the importance of information systems security and the possible negative effects of a security breach or failure. During an awareness campaign, the end user simply receives information. It is designed to reach a broad audience using various promotional techniques. In a training environment, the student is expected to be an active participant in the process of acquiring new insights, knowledge, and skills. When designing and developing an information technology (IT) security training program, there is a wide range of options that are based on specific job requirements and the daily management, operation, and protection of information systems.

IT is apparent in every aspect of our daily life — so much so that in many instances, it seems completely natural. Can you imagine conducting business without e-mail or voice mail? How about hand-writing a report that is later typed using an electric typewriter? As one is well aware, computer technology and open-connected networks are the core com-
ponents of all organizations, regardless of the industry or the specific business needs.

Information technology has enabled organizations in the government and private sectors to create, process, store, and transmit an unprecedented amount of information. The IT infrastructure created to handle this information flow has become an integral part of how business is conducted. In fact, most organizations consider themselves dependent on their information systems. This dependency on information systems has created the need to ensure that the physical assets (e.g., the hardware and software) and the information they process are protected from actions that could jeopardize the ability of the organization to effectively perform official duties.

Several IT security reports estimate that if a business does not have access to its data for more than ten days, it cannot financially recover from the economic loss.

While advances in IT have increased exponentially, very little has been done to inform users of the vulnerabilities and threats of the new technologies. In March 1999, Patrice Rapalus, Director of the Computer Security Institute, noted that “corporations and government agencies that want to survive in the ‘Information Age’ will have to dedicate more resources to staffing and training of information system security professionals.” To take this a step further, not only must information systems security professionals receive training, but all employees who have access to information systems must be made aware of the vulnerabilities and threats to the IT system they use and what they can do to help protect their information.

Employees — especially end users of the IT system — are typically not aware of the security consequences caused by certain actions. For most employees, the IT system is a tool to perform their job responsibilities as quickly and efficiently as possible; security is viewed as a hindrance rather than a necessity. Thus, it is imperative for every organization to provide employees with IT-related security information that points out the threats and ramifications of not actively participating in the protection of their information. In fact, federal agencies are required by law (Computer Security Act of 1987) to provide security awareness information to all end users of information systems.

Employees are one of the most important factors in ensuring the security of IT systems and the information they process. In many instances, IT security incidents are the result of employee actions that originate from inattention and not being aware of IT security policies and procedures. Therefore, informed and trained employees can be a crucial factor in the effective functioning and protection of information systems. If employees are aware of IT security issues, they can be the first line of defense in the prevention and early detection of problems. In addition,
when everyone is concerned and focused on IT security, the protection of assets and information can be much easier and more efficient.

To protect the confidentiality, integrity, and availability of information, organizations must ensure that all individuals involved understand their responsibilities. To achieve this, employees must be adequately informed of the policies and procedures necessary to protect the IT system. As such, all end users of information systems must understand the basics of IT security and be able to apply good security habits in the daily work environment. After receiving commitment from senior management, one of the initial steps is to clearly define the objective of the security awareness program. Once the goal has been established, the content must be decided, including the type of implementation (delivery) options available. During this process, key factors to consider include how to overcome obstacles and face resistance. The final step is evaluating success; and this article now focuses on the steps in developing an IT security awareness program.

SETTING THE GOAL

Before beginning to develop the content of a security awareness program, it is essential to establish the objective or goal. It may be as simple as “all employees must understand their basic security responsibilities” or “develop in all employees an awareness of the IT security threats the organization faces and motivate the employees to develop the necessary habits to counteract the threats and protect the IT system.” Some may find it necessary to develop something more detailed, such as:

**Awareness Program Objectives**

Employees must be aware of:

- threats to physical assets and stored information
- threats to open network environments
- federal laws they are required to follow, such as copyright violations or privacy act information
- specific organization or department policies they are required to follow
- how to identify and protect sensitive (or classified) information
- how to store, label, and transport information
- who they should report security incidents to, regardless of whether it is just a suspected or an actual incident
- e-mail/Internet policies and procedures

When establishing the goals for the security awareness program, keep in mind that these goals should reflect and support the overall mission and goals of the organization. At this point in the process, it may be the right (or necessary) time to provide a status report to the Chief Information Officer (CIO) or other executive/senior management members.
DECIDING ON THE CONTENT
An IT security awareness program should create sensitivity to the threats and vulnerabilities of IT systems and also remind employees of the need to protect the information they create, process, transmit, and store. Basically, the focus of an IT security awareness program is to raise the security consciousness of all employees.

The level and type of content depends on the needs of the organization. Essentially, employees need to be told what they need to protect, how they should protect it, and how important IT systems security is to the organization.

IMPLEMENTATION (DELIVERY) OPTIONS
The methods and options available for delivering security awareness information are very similar to those used for delivering other employee awareness information (e.g., sexual harassment or business ethics). And although this is true, it may be time to break with tradition and step out of the box — in other words, it may be time to try something new.

Think of positive, fun, exciting, and motivating methods that will give employees the message and encourage them to practice good computer security habits. Keep in mind that the success of an awareness program is its ability to reach a large audience through several attractive and engaging materials and techniques. Examples of IT security awareness materials and techniques include:

- posters
- posting motivational and catchy slogans
- videotapes
- classroom instruction
- computer-based delivery, such as CD-ROM or intranet access
- brochures/flyers
- pens/pencils/keychains (any type of trinket) with motivational slogans
- post-it notes with a message on protecting the IT system
- stickers for doors and bulletin boards
- cartoons/articles published monthly or quarterly in in-house newsletter or specific department notices
- special topical bulletins (security alerts in this instance)
- monthly e-mail notices related to security issues or e-mail broadcasts of security advisories
- security banners or pre-logon messages that appear on the computer monitor
- distribution of food items as an incentive. (For example, distribute packages of the gummy-bear type candy that is shaped into little snakes. Attach a card to the package, with the heading “Gummy Virus Attack at XYZ.” Add a clever message such as: “Destroy all virus-
es wiggling through the network — make sure your anti-virus software is turned on.”)

The Web site http://awarenessmaterials.homestead.com/ lists the following options:

• First Aid Kit with slogan: “It’s healthy to protect our patient’s information, it’s healthy to protect our information.”
• Mirror with slogan: “Look who is responsible for protecting our information.”
• Toothbrush with slogan: “Your password is like this toothbrush: use it regularly, change it often, and do not share it with anyone else.”
• Badge Holder (retractable) with slogan: “Think Security”
• Key-shaped magnet with slogan: “You are the key to good security!”
• Flashlight with slogan: “Keep the spotlight on information protection.”

Another key success factor in an awareness program is remembering that it never ends — the awareness campaign must repeat its message. If the message is very important, then it should be repeated more often, and in a different manner each time. Because IT security awareness must be an ongoing activity, it requires creativity and enthusiasm to maintain the interest of all audience members. The awareness materials should create an atmosphere that IT security is important not only to the organization, but also to each employee. It should ignite an interest in following the IT security policies and rules of behavior.

An awareness program must remain current. If IT security policies are changing, the employees must be notified. It may be necessary and helpful to set up technical means to deliver immediate information. For example, if the next “lovebug” virus has been circulating overnight, the system manager could post a pre-logon message to all workstations. In this manner, the first item the users see when turning on their workstations is information on how to protect the system, such as what to look for and what not to open.

Finally, the security awareness campaign should be simple. For most organizations, the awareness campaign does not need to be expensive, complicated, or overly technical in its delivery. Make it easy for employees to get the information and make it easy to understand.

Security awareness programs should (be):

• supported and led by example from management
• simple and straightforward
• positive and motivating
• a continuous effort
• repeat the most important messages
• entertaining
• humorous where appropriate — make slogans easy to remember
• tell employees what the threats are and their responsibilities for protecting the system

In some organizations, it may be a necessary (or viable) option to outsource the design and development of the awareness program to a qualified vendor. To find the best vendor to meet an organization’s needs, one can review products and services on the Internet, contact others and discuss their experiences, and seek proposals from vendors that list previous experiences and outline their solutions to your goals.

OVERCOMING OBSTACLES
As with any employee-wide program, the security awareness campaign must have support from senior management. This includes the financial means to develop the program. For example, each year management must allocate dollars that will support the awareness materials and efforts. Create a project plan that includes the objectives, cost estimates for labor and other materials, time schedules, and outline any specific deliverables (i.e., 15-minute video, pens, pencils, etc.). Have management approve the plan and set aside specific funds to create and develop the security awareness materials.

Keep in mind that some employees will display passive resistance. These are the employees who will not attend briefings, and who will create a negative atmosphere by ignoring procedures and violating security policies. There is also active resistance, wherein an employee may purposefully object to security protections and fight with management over policies. For example, many organizations disable the floppy drive in workstations to reduce the potential of viruses entering the network. If an employee responds very negatively, management may stop disabling the floppy drives. For this reason, it is important to gain management support before beginning any type of security procedures associated with the awareness campaign.

Although there will be resistance, most employees (this author is convinced it is 98 percent) want to perform well in their jobs, do the right thing, and abide by the rules. Do not let the nay-sayers affect security efforts — computer security is too important to let a few negative people disrupt achieving good security practices for the organization.

Frustrated at this point? It is common for companies to agree to an awareness program but not allocate any human or financial resources. Again, do not be deterred. Plan big, but start small. Something as simple as sending e-mail messages or putting notices in the newsletter can be a cost-effective first step. When management begins to see the effect of the awareness material (of course they will notice — you will be pointing them out), then the needed resources may be allocated. The important
thing is to keep trying and doing all that one can with the available re-
resources (or lack of them).

Employees are the single, most important asset in protecting the IT
system; and users who are aware of good security practices can ensure
that information remains safe and available.

Check out the awareness tip from Mike Lambert, CISSP, on his Web
directions and information are provided on how to develop “pop-up an-
nouncements.” A great idea!

EVALUATION

All management programs, including the security awareness program,
must be periodically reviewed and evaluated. In most organizations there
will be no need to conduct a formal quantitative or qualitative analysis.
It should be sufficient to informally review and monitor whether behav-
iors or attitudes have changed. The following provides a few simple op-
tions to consider.

1. Distribute a survey or questionnaire seeking input from employees.
   If an awareness briefing is conducted during the new-employee ori-
   entation, follow up with the employee (after a specified time period
   of three to six months) and ask how the briefing was perceived (i.e.,
   what do they remember, on what would they have liked more infor-
   mation, etc.).

2. While pouring a cup of coffee in the morning, ask others in the room
   about the awareness campaign. How did they like the new poster?
   How about the cake and ice cream during the meeting? Remember:
   the objective is to heighten the employee’s awareness and responsi-
   bilities of computer security. Thus, even if the response is, “That post-
   er is silly,” do not fret; it was noticed and that is what is important.

3. Track the number and type of security incidents that occur before
   and after the awareness campaign. Most likely, it is a positive sign if
   there is an increase in the number of reported incidents. This is an
   indication that users know what to do and who to contact if they sus-
  pect a computer security breach or incident.

4. Conduct “spot checks” of user behavior. This may include walking
   through the office, checking to see if workstations are logged in
   while unattended or if sensitive media are not adequately protected.

5. If delivering awareness material via a computer-based delivery (e.g.,
   loading it on the organization’s intranet), record user names and
   completion status. On a periodic basis, check to see who has re-
   viewed the material. One could also send a targeted questionnaire to
   those who have completed the online material.

6. Have the system manager run a password-cracking program against
   the employees’ passwords. If this is done, consider running the pro-
gram on a stand-alone computer and not installing it on the network. Usually, it is not necessary or desirable to install this type of software on a network server. Beware of some free password-cracking programs available from the Internet because they may contain malicious code that will export a password list to a waiting hacker.

Keep in mind that the evaluation process should reflect and answer whether or not the original objectives/goals of the security awareness program have been achieved. Sometimes, evaluations focus on the wrong item. For example, when evaluating an awareness program, it would not be appropriate to ask each employee how many incidents have occurred over the past year. However, it would be appropriate to ask each employee if he or she knows whom to contact if a security incident is suspected.

SUMMARY
Employees are the single, most important aspect of an information system security program, and management support is the key to ensuring a successful awareness program.

The security awareness program needs to be a line item in the information system security plan. In addition to the operational and technical countermeasures that are needed to protect the system, awareness (and training) must also be an essential item. Various computer crime statistics show that the threat from insiders ranges from 65 to 90 percent. This is not an indication that 60 percent of the employees in an organization are trying to hack into the system; it does mean that employees, whether intentionally or accidentally, may allow some form of harm to the system. This includes loading illegal copies of screen-saver software, downloading shareware from the Internet, creating weak passwords, or sharing their passwords with others. Thus, employees need to be made aware of the IT system “rules of behavior” and how to practice good computer security skills. Further, in federal organizations, it is a law (Computer Security Act of 1987) that every federal employee must receive security awareness training on an annual basis.

The security awareness program should be structured to meet the organization’s specific needs. The first step is to decide on the goals of the program — what it should achieve — and then to develop a program plan. This plan should then be professionally presented to management. Hopefully, the program will receive the necessary resources for success, such as personnel, monetary, and moral support. In the beginning, even if there are not enough resources available, start with the simple and no-cost methods of distributing information. Keep in mind that it is important just to begin; and along the way, seek more resources and ask for assistance from key IT team members.
The benefit of beginning with an awareness campaign is to set the stage for the next level of IT security information distribution, which is IT security training. Following the awareness program, all employees should receive site-specific training on the basics of IT security. Remember that awareness does not end when training begins; it is a continuous and important feature of the information system security awareness and training program.

Susan D. Hansche, CISSP, is a senior manager for information system security awareness and training at TROY Systems, Inc., based in Fairfax, Virginia. She has designed numerous training courses on information technology and information systems security for both private-sector and government clients. She can be reached via e-mail at shanske@troy.com.