Information Systems Security
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uiss19

Designing a Security Awareness Program: Part 1

Susan Hansche CISSP [a]

[a] 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 system security for both private sector and government clients. She can be reached via e-mail at shansche@troy.com

Published online: 21 Dec 2006.

To cite this article: Susan Hansche CISSP (2001) Designing a Security Awareness Program: Part 1, Information Systems Security, 9:6, 1-9, DOI: 10.1201/1086/43298.9.6.20010102/30985.4

To link to this article: http://dx.doi.org/10.1201/1086/43298.9.6.20010102/30985.4

Designing a Security Awareness Program: Part I

Susan Hansche, CISSP

This article represents the first of a two-part series on the importance of providing both security awareness and information systems security training to all employees, regardless of their job responsibilities. In this first article, the focus is on the first step of providing computer and information system security—developing and implementing an effective security awareness program. Readers may ask why security awareness is not considered the same as training. The simple answer is 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.

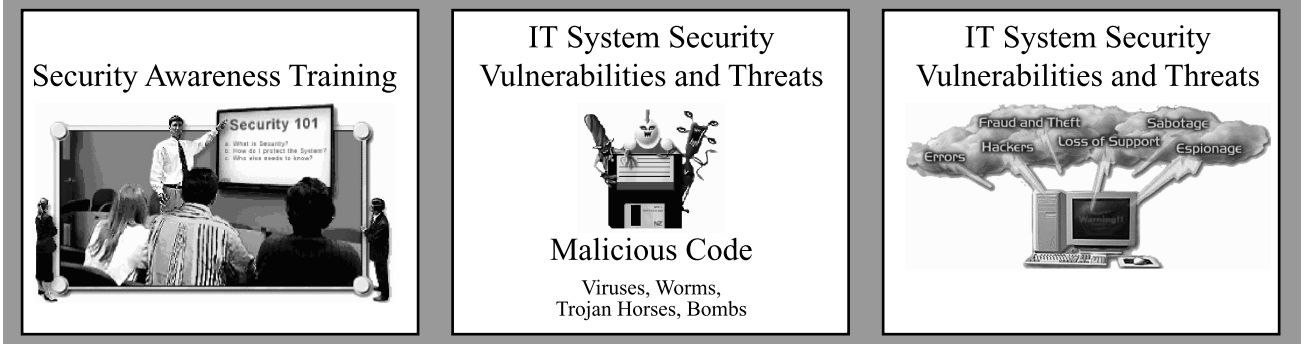
When designing and developing an information technology (IT) security training program, there is a wide range of options that are based on specific job requirements and the daily management, operation, and protection of the information system. The second article, therefore, will describe a framework to help organizations determine the most efficient and economical solutions for their training needs.

INTRODUCTION

Information technology (IT) is apparent in every aspect of our daily lives—so much so that in many instances, it seems completely natural. Imagine conducting business without e-mail or voice mail—or handwriting a report that is later typed using an electric typewriter. Clearly, computer technology and open-connected networks are the core components of all organizations, regardless of the industry or the specific business needs.

Information technology has enabled

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 system security for both private sector and government clients. She can be reached via e-mail at shansche@troy.com.



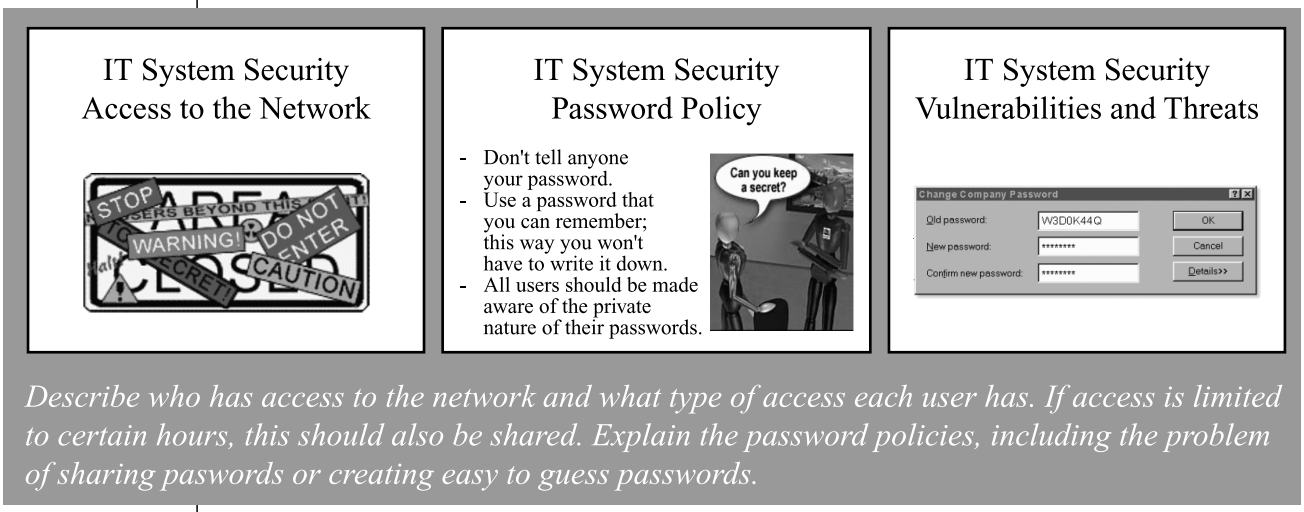
Identify and describe the IT system's vulnerabilities and the type of threats that could harm the system.

organizations in the federal 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—such as 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 10 days, it cannot financially recover from the economic loss. While advances in information technology (IT) have increased exponentially, very little has been done to inform users of the vulnerabilities and threats of the new technologies. In March of 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 every employee who has access to the information system 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



Describe who has access to the network and what type of access each user has. If access is limited to certain hours, this should also be shared. Explain the password policies, including the problem of sharing paswords or creating easy to guess passwords.

trained employees can be a crucial factor to the effective functioning and protection of the information system. 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.

In order 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 the information system must understand the basics of IT security and be able to apply good security habits in their daily work environment. After receiving commitment from senior management, one of the initial steps is clearly defining 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 are how to overcome obstacles and face resistance. The final step is evaluating success. The discussion focuses on these steps of developing an IT security awareness program. The first step in any IT security awareness program is to obtain a commitment from executive management.

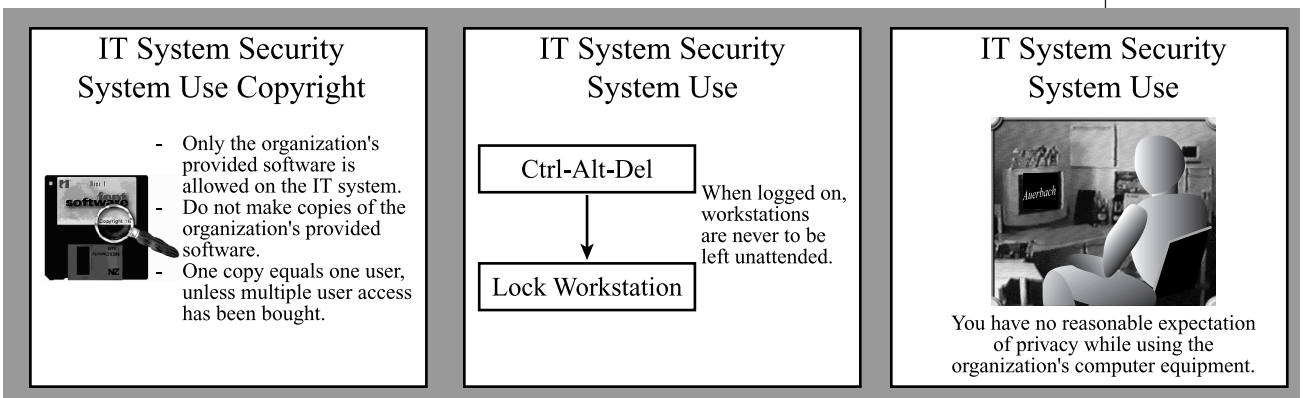
SETTING THE GOAL

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 each employee 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:

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 sensi-



Define the system use policies, such as installing software, copyright issues, and leaving the workstation logged on when unattended. Included in ths could be the user's expectation of privacy on the system.

tive (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 and Internet policies and procedures

When establishing the goals for the security awareness program, keep in mind that they 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 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.

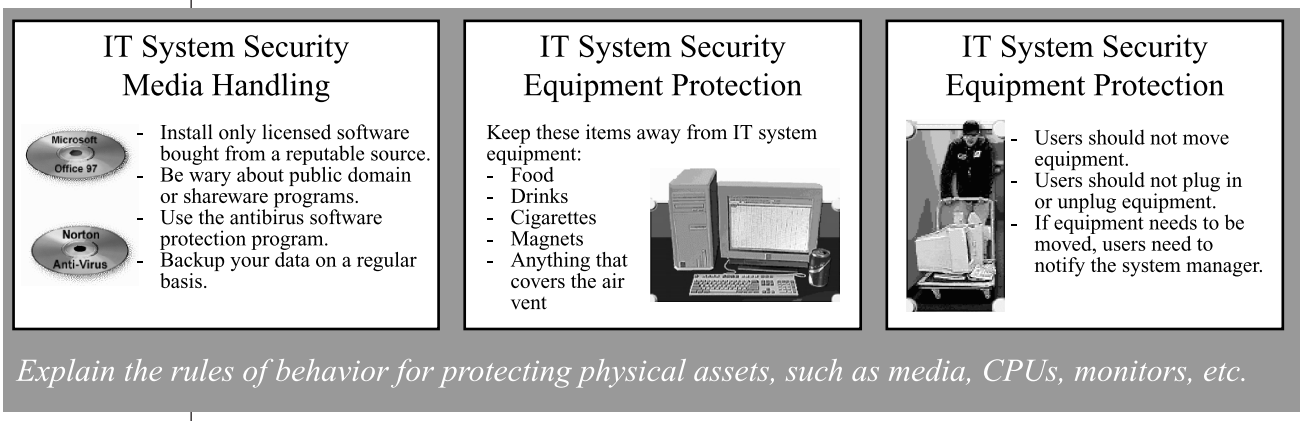
The level and type of content is dependent on the needs of the organization. Essentially, management needs to tell employees what they need to protect, how they should protect it, and how important IT system security is to the organization.

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, such as sexual harassment or business ethics. Even though 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. Example of IT security awareness materials and techniques include:

☐ Posters
☐ Posting of motivational and catchy slogans
☐ Videotapes
☐ Classroom instruction
☐ Computer-based delivery, such as



Explain the rules of behavior for protecting physical assets, such as media, CPUs, monitors, etc.

CD-ROM or intranet access
☐ Brochures and flyers
☐ Pens, pencils, and 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 or articles published monthly or quarterly in the 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
☐ A security banner or pre-logon message that appears on the computer monitor.
☐ Distribute 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 viruses wiggling through the network—make sure your antivirus 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 materials should create an awareness that IT security is important not only to the organization, but also to each employee. They 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 a technical means to deliver immediate information. For

Are there specific laptop policies? How about telecommuting? Are there specific policies for e-mail or Internet use? It may be necessary to inform users about the threats to each of these types of access.

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 the machine 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):

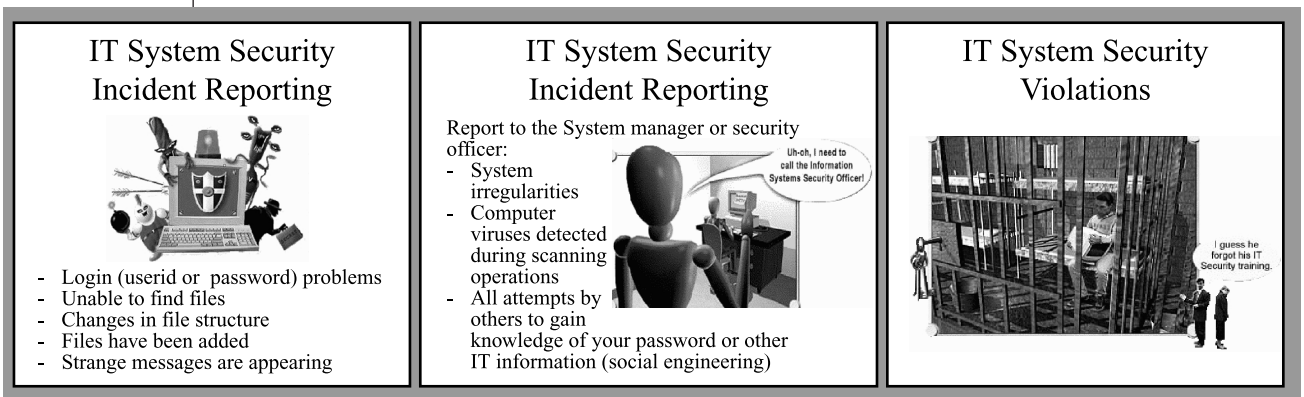
☐ Supported and led by example from management
☐ Simple and straightforward
☐ Positive and motivating
☐ A continuous effort
☐ Repeat the most important messages
☐ Entertaining
☐ Humorous where appropriate—make slogans easy to remember
☐ Tell employees what the threats are and their responsibilities for 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 the organization's needs, managers 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 for achieving the organization's goals.

OVERCOMING OBSTACLES

As with any companywide 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, and time schedules, and outline any specific deliverables (i.e., 15-minute video, pens, pencils). 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 fail to attend briefings and create a negative atmosphere by ignoring procedures and violating security policies. There is also active resistance; an employee may purposefully object to security protec-



Clearly define what type of computer security incidents need to be reported and to whom. Explain the consequences that each user will face if they violate the computer security policies.

tions and fight with management over policies. For example, many organizations disable the floppy drive in workstations to reduce the potential for viruses to enter the network. If an employee responds very negatively, management may stop disabling the floppy drives. For this reason, management support is important to obtain before beginning any type of security procedure associated with the awareness campaign.

Even though there will be resistance, most employees (probably 98 percent) want to perform well in their job, do the right thing, and abide by the rules. Do not let the naysayers affect the effort; computer security is too important to let a few negative people disrupt achieving good security practices for the organization.

It is common for companies to agree to an awareness program but not allocate any human or financial resources. Security managers should 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—security staff will be pointing them out), then the needed resources may be allocated. The important thing is to keep trying and do everything possible with current resources (or lack of them).

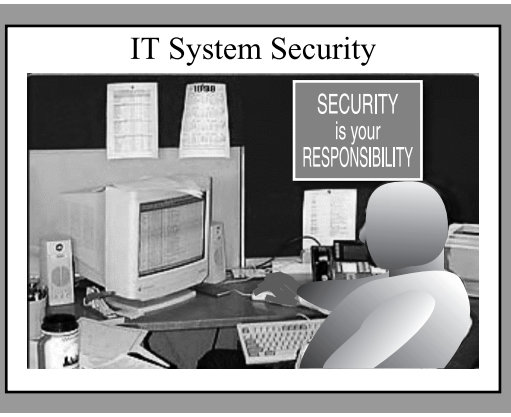
Employees are the single most important asset in protecting the IT system; users who are aware of good security practices can ensure that information remains safe and available. Check out the awareness tip from Mike Lambert, CISSP, on his web page: http://www.frontiernet.net/~mlambert/awareness/. Step-by-step directions and information are provided on how to develop "pop-up announcements."

EVALUATION

All management programs, including the security awareness program, must be periodically reviewed and evaluated. In most organizations there will not be a need to conduct a formal quantitative or qualitative analysis. It should be sufficient to informally review and monitor whether behaviors or attitudes have changed. The following list details a few simple options to consider:

□ Distribute a survey or questionnaire seeking input from employees. If an awareness briefing is conducted during the new-employee orientation, follow up with the employees (after a specified time period of three to six months) and ask how the briefing

Explain the importance of each user following the rules of behavior--so that their information will always be available, and remain accurate and confidential.



End on a high note. Be positive, motivating, and encouraging. This is a good time to distribute the awareness trinkets: pens, pencils, coffee mugs, magnets, t-shirts (or, even better, polo shirts to wear on casual Fridays).

was perceived (i.e., what do they remember, what would they have liked more information on).

☐ 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 that the objective is to heighten the employees' awareness and responsibilities of computer security. Thus, even if the response is "that poster is silly," do not fret; it was noticed and that is what is important.

☐ 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 whom to contact if they suspect a computer security breach or incident.

☐ Conduct "spot checks" of user behavior. This may include walking through the office checking whether workstations are logged in while unattended or sensitive media are not being adequately protected.

☐ If delivering awareness material via a computer-based delivery, such as loading it on the organization's intranet, record student names and completion status. On a periodic basis, check to see who has reviewed the material. In addition, send a targeted questionnaire to those who have completed the on-line material.

☐ Have the system manager run a password-cracking program against the employee's passwords. To do this, consider running the program 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 the network server. Beware of some free password-cracking programs available from the Internet, because they may contain malicious code that will export the firm's password list to a waiting hacker.

Keep in mind that the evaluation process should determine whether the original goals of the security awareness program were 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 last year. However, it would be appropriate to ask all employees whether they know whom to contact if they suspect a security incident.

CONCLUSION

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 organization's information system security

plan. In addition to the operational and technical countermeasures that are needed to protect the system, awareness (and training) must 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 the organization are trying to hack into the system; it does mean 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.

The security awareness program should be structured to meet your organization's specific needs. The first step is deciding on the goals of the program—what it should achieve—and then developing a program plan. This plan should then be professionally presented to management. Hopefully, the program will receive the necessary resources for success—personnel, funding, 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. ■