



Chapter 29

Security Awareness

**K Rudolph, CISSP,
Gale Warshawsky, and
Louis Numkin**

1 Awareness as a Survival Technique

An organization's staff is the most cost-effective countermeasure against security violations. They are generally the first to be impacted by security incidents, and their compliance with security policy can make or break a security program. A staff that is aware of security concerns can prevent incidents and mitigate damage when incidents do occur. Given the importance of the staff as a security control, awareness is therefore the most important part of an organization's security program.

Experts recommend that 40 percent of an organization's security budget be spent on awareness¹ measures. In the animal kingdom, awareness - being alert to danger signals and responding quickly - can be the difference between surviving and not. This is also true for organizations. Bats and dolphins use sonar to detect and avoid dangers, and cats use whiskers and keen senses of hearing, smell, and night-vision to probe their environments. Personnel who have developed an awareness of danger signals can function as an organization's sensitive detection instruments. Recognition of events that could indicate a security incident should be a reflex. Awareness activities can build this reflexive behavior.

This chapter provides information on security awareness programs. It addresses:

- Critical success factors
- An approach for developing an awareness program
- Principles of awareness
- Content
- Techniques
- Tools
- Measurement and evaluation
- Resources.

2 Critical Success Factors

An organization's security awareness program needs a successful launch for maximum impact. An Awareness Program Pre-flight Checklist can help ensure a successful launch. The Checklist makes sure that the critical program elements listed below are not overlooked:

- Information security policy
- Senior level management support and buy-in
- Awareness program focus that security, at its core, is a people problem
- Goals (short term, intermediate, and long range)
- Audience profiles
- Incorporation of motivational techniques.

2.1 In place Information Security Policy

Security is important and should be addressed by policies that clarify and document management's intention. Policies are an organization's "law." They set employee expectations and guide behaviors. An effective information security policy includes statements of goals and responsibilities and clearly details what activities are allowed, what activities are not allowed, and what penalties may be imposed for failure to comply.

Information security policies indicate that management wishes to focus attention on security. In addition to saying, "This is important, pay attention," well-defined security policies make it easier to take disciplinary action and prosecute those who compromise security. Established policies are also useful in dealing with personality types who will not do something until "management tells me to."

An information security awareness policy gives the information security program credibility and visibility. It shows that management believes that security is important and everyone will be held accountable for his or her actions.

An awareness policy should establish three things:

- 1) That participation in an awareness program is required for everyone, including contractors or other outsiders who have access to information systems. The policy should address new arrivals and existing employees. For example, new arrivals might be required to receive an information security awareness briefing within a specific timeframe (e.g., 60 days after hire²) or before being allowed system access. Existing employees might be required to attend an awareness activity or take a course within 3 months of program initiation and periodically thereafter (e.g., quarterly or annually). Existing employees might also be required to refresh their security awareness when the organization's information technology environment changes significantly or when the employee enters a new position that deals with sensitive data.
- 2) That everyone will be given sufficient time to participate in awareness activities. In many organizations, policy also states that people will be asked to sign a statement indicating that they understand the material presented and will comply with security policies.
- 3) Who is responsible for conducting awareness program activities. The program might be created and implemented by one or a combination of: the training department; the security staff; or an outside organization, consultant, or security awareness specialist.

2.2 Senior Level Management Support

Senior management must be committed to information security. It must visibly demonstrate that commitment by setting an example of security awareness, by providing an adequate budget, and by supporting the security staff.

2.2.1 Budget

Demonstrated, documented top-management support prevents middle managers from denying requests to fund information security. Managers often do not allocate employee time for security awareness activities because they do not see a direct connection between them and the “bottom line” for which they are held accountable.

2.2.2 Example

Senior management must lead by example. If senior managers do not take security seriously, the program will lack credibility. For example, if the security policy prohibits employees from bringing software from home for use on the organization’s PCs, and senior executives are seen using such software to evaluate their portfolios, employees will perceive the policy as inconsistent, unfair, and not universally applicable.

2.2.3 Security staff backing

Senior managers should be prepared to stand behind the organization’s policies and the security staff charged with enforcing compliance. This is especially important in areas where security and convenience conflict, such as enforcing a control that removes system access for users whose records do not show that they have completed an awareness refresher during the previous year.

2.3 Information Security is a People Problem

As early as 1952, UNIVAC, the first commercial computer, was used to predict the outcome of the U.S. presidential election. The human operators refused to believe its prediction, a landslide for Eisenhower, so they reprogrammed it to come up with a different solution. The actual result was, in fact, a landslide for Eisenhower. This caused some to declare that, “The trouble with machines is people.”

Many technical people view computer security as a technology problem. They use sophisticated hardware and software solutions to control access and prevent fraud. The reality is that computer security is a people problem. Connecting computers into networks significantly increases risk, and network security depends heavily on the cooperation of each and every user. Security is only as strong as the weakest link, and authorization and identification controls are useless if even one user does not recognize the value of the information assets that are to be protected, and allows the system to be compromised.

2.4 Goals

“Sighted sub. Sank same.”

- David Francis Miller, U.S. Navy Pilot, Radio Message, February 26, 1942

Ideally, the goals of an awareness program should be similar to the one reported on by Pilot Miller: specific, realistic, and measurable. Measuring awareness can be challenging and is covered in greater detail in section 29.8. An effective awareness program reinforces desired behaviors and gradually changes undesired behaviors.

Employees usually know much of what an awareness program conveys, but the program serves to reinforce this knowledge, and to produce security behaviors that are automatic. One goal of an information security awareness program, therefore, could be to make “thinking security” a natural reflex for everyone in the organization. Just as martial artists practice many hours to reinforce techniques until they become automatic responses, awareness programs use repetition to reinforce desired behaviors and attitudes about security.

Another might be to set the stage for training by impressing upon users the importance of information security, and the adverse consequences of its failure. Training involves teaching knowledge and skills to individuals so that they can perform more effectively. Training is more comprehensive and detailed than awareness activities.

2.5 Audience Profiles

A U.S. Critical Infrastructure Assurance Office publication states: “The level of security awareness required of a summer intern program assistant is the same as that needed by the Director, Chief, or Administrator of the agency.”³ This may be true, but the methods for effectively reaching those people with the awareness message may need to be different. It is easier to hit the bull’s eye when one can focus on a specific target.

Several different audiences exist within most organizations, with characteristics based on their needs, roles, and interests.

- **Needs.** Audiences with similar needs will have similar levels of computer knowledge and experience. End users with minimal computer experience may be intimidated by, and will not respond well, to jargon. Analogies and examples are more appropriate for audiences with little in-depth computer expertise.
- **Roles and interests.** End users are usually interested in getting their job done with as little obstruction as possible. They are usually interested in knowing about the effect of security on their workload, delays, and job performance evaluations. Managers are usually interested in the bottom line and measurable results. They want to know, “How much will this security control cost?” and “What kind of return on the investment will it bring?” Technical staff should receive materials with correct technical terms. Otherwise, they may conclude that the information is beneath them or that it has been prepared by people without technical knowledge.

To create an awareness program, identify the audiences and conduct research to find out what the audiences know and what questions about security they ask most often. Surveys and questionnaires can be used to reveal the starting level of awareness of security issues. This will be useful for measuring progress after the awareness program is implemented.

Historical information can also provide clues as to what the audience knows and does not know. Asking, “What security-related problems has the organization experienced?” may reveal information that can be used to tailor the awareness program.

2.6 The Art of Motivation

An awareness program may seek to change attitudes and behaviors that are ingrained habits or that have emotional significance that makes them hard to change. To overcome this resistance, an awareness program must appeal to other attitudes or preferences. For example, a person who believes that it is acceptable to share another individual's personal data with a coworker, or a password with a new hire who has not been approved for system access, must be shown that people are respected and recognized in the organization for protecting confidential data rather than sharing it.

As long as people associate hackers with being "cool," an awareness program is not likely to impress them with anti-hacker messages. Instead, the message should emphasize something that will appeal to the audience, for example, the damage done when a person's identity or personal data is stolen and that person cannot get a loan or health insurance five years later. An awareness program should deglamorize hackers by focusing on the victims and the harmful results of their activities. People need to be made aware that hackers hurt people, whether they intend to or not.

Messages that call for controls that result in inconvenience, or that require a sacrifice by the audience may not be perceived well. A hostile environment for security can result from people having to comply with cumbersome controls while management is demanding greater productivity.

Another factor in motivation is, "How sensitive are the audience members to the opinions of others?" If the audience is mostly new hires and young people, the message can capitalize on the idea that young people often want to belong. People pass chain letters on because they are superstitious or want the acceptance of being part of the group that has seen the latest Internet humor. If someone receives an e-mail attachment with an interesting subject, there is pressure to open it and respond. The awareness program needs to establish a value in belonging to a group that shuns such harmful activity.

The right message will have a positive spin. Instead of glamorizing the independence of the hackers, the message should emphasize the courage and independence it takes to resist appeals from friends and co-workers to share copyrighted software. Withstanding peer pressure to make unethical or risky choices can be shown in a positive light, so that the people who follow the rules are seen as praiseworthy and not as wimps.

Fear can be an effective motivator, but the primary value of scare tactics is to get the user community to start thinking about security in a new way. Fear-based messages are most effective for motivation when the message includes information on how to avoid or protect oneself from danger.

Potential pitfalls of awareness programs that are not carefully designed include the dangers of:

- Losing the audience's attention,
- Alienating the audience, and
- Over-doing it.

An awareness program is like an exercise program. If the audience is bombarded with everything in the awareness arsenal at once, they may become overwhelmed and will not stick

with the program. It is important that management understand that effective awareness programs are long-term activities that bring gradual improvement.

3 Approach

3.1 Media Campaign

Raising awareness is similar to commercial advertising or social marketing, such as the campaigns to reduce smoking or decrease the use of alcohol on college campuses. In the security awareness campaign, the message is the need for security, the product to be sold is the practice of security, and the market is all employees. Communication is the essential tool and the information disseminated becomes the foundation on which behavioral change is built. Research and planning are essential and should result in a clear strategy that includes the following:

- Definition of program objectives
- Identification of primary and secondary audiences
- Definition of information to be communicated
- Description of benefits as perceived by the audience

Research can be conducted by observation, surveys, tests, and interviews. Help desk statistics and trends should be reviewed for indications of actual and potential security incidents. A large number of calls for password resets might indicate that password procedures need review or that users need additional training. Ask the staff how they would break into the system; the people closest to the system ought to know its vulnerabilities. Ask the staff to consider questions such as, "Are security breaches predictable?"

Another similarity between commercial advertising and awareness programs is the importance of pre-testing materials before distributing them. This can be done with focus group interviews, with in-depth individual interviews, and with interviews where multiple choice or closed-ended questions are used to allow quick responses.

3.2 Is a Plan Necessary? Sharpening the Ax

Abraham Lincoln has been quoted as saying that if he had six hours to chop down a tree, he would spend the first five sharpening the ax. Planning is like sharpening an ax, so that awareness materials can be carefully designed to get specific, positive responses.

The security awareness plan can be as short as 3 to 5 pages, and should identify:

- The status of the organization's current efforts,
- Program goals and objectives, and how progress will be measured, and
- Actions (with associated dates) that will be taken and by whom.

Plans allow for faster reaction and enable organizations to take advantage of current events in the news. Planning also allows coordination around a theme.

4 Awareness Principles – ABCs

4.1 “A”

Attention-Getting

Attention is a prerequisite to learning. Awareness activities and materials should be designed to get attention in a positive way. Clever slogans and eye-catching images contribute to the program's success.

Appeal to Target Audience

Awareness programs that appeal to the existing values and motivations of the target audience will be more successful than ones that try to change them.

4.2 “B”

Basic - Keep it Simple and Memorable

Awareness efforts should be simple. Awareness sets the stage for training, but is not intended to be complex. An objective of an awareness program might be to take away the fear and ignorance that has traditionally surrounded information security. Awareness is intended to make people recognize that there is a problem and that they are part of the solution.

Buy-in is Better than Coercion

People who have contributed to the awareness program with suggestions, contest entries, or focus-group testing are more likely to accept and follow security controls. This assumes that there is feedback for every suggestion submitted. No feedback implies “no management interest.”

4.3 “C”

Current

Awareness material must be fresh and not stale. Chef Oscar Gizelt of Delmonico's Restaurant in New York said, “Fish should smell like the tide. Once they smell like fish, it's too late.” If awareness material is not changed frequently, it, too, begins to smell old and becomes boring.

Credible

Credibility is crucial for an awareness program to be effective. The message should be clear, relevant, and appropriate to the real world. If the audience is required to use 15 different passwords as a part of day-to-day functions, prohibiting them from writing their passwords may not be as realistic as providing strategies for protecting the written list.

Continuing

Security awareness programs are long-term efforts and require persistence. Repetition is important and so is variety of the method by which the message is delivered.

5 Content

What should an awareness program address? Below are some suggestions for the minimum topics.

5.1 Risks

All organization members need to be able to answer the question, “What does a threat look like?” Awareness material should address how unauthorized activity might appear on local systems. For example, system users might be taught to recognize that a repeated busy signal on an 800 line could be caused by busy circuits or it could be a cracker trying to break in. Specific items that apply to most awareness programs include:

- “Malware” (e.g., malicious mobile code, viruses, and worms) and how it can damage an information system,
- The principle of shared risk in networked systems, where a risk assumed by one is imposed on the entire network,
- The impact of distributed attacks and distributed denial of service attacks,
- Privacy issues (including vulnerability of payroll, medical, and personnel records), and
- The scope of embedded software and hardware vulnerabilities and how the organization corrects them.

The material should be tailored to the needs of the audience. For example, if employees use home computers or laptops to connect to the organization’s networks, then the material should address the risks associated with remote access.

5.2 Basic Countermeasures

The next step after getting employees to recognize a security problem is making them aware of how they should react to an incident. This would include:

- Procedures for using information technology systems in a secure manner.
- Personal practices to ensure compliance with applicable policy, for example password creation and management, handling e-mail attachments, and file transfers and downloads.
- Procedures for reporting potential or actual security events, specifically “who to” and “how to” report unauthorized or suspicious activity. For example, in some situations the telephone is more appropriate than e-mail. This would be indicated if a user suspects that a system is under attack and the attacker may be monitoring e-mail.

5.3 Responsibilities

The awareness program should emphasize that security is everyone's responsibility, that management has made it a priority, and that it applies to everyone in the organization equally. System or organization-specific Rules or Codes of Behavior should be promulgated so that all employees know exactly what to do, and what is expected of them.

5.4 Contact Information

Another key component of material to be presented is contact information for incident reporting, for asking non-emergency security questions, and for making suggestions. People must be made aware of: who, how, what, and when.

- Who: Contact information, such as telephone and pager numbers, e-mail, and web site URLs (addresses) should be provided for security staff, the incident response team, and help desk personnel.
- What: The types of information that will be needed to report a suspected problem, for example:
 - Affected system(s) or site(s)
 - Hardware and operating system
 - Symptoms
 - Date, time, and duration of incident
 - Connections with other systems that were active
 - Actions taken
 - Damage
 - Assistance needed
- How: Instructions for reporting suspected problems by telephone or by e-mail using a system that is not suspected of being under attack.
- When: Users need to know in what sorts of situations time is of the essence. If immediate reporting can prevent further damage, users should know not to delay.

6 Techniques

Presentation of awareness materials is crucial. If the employee's reaction is, "I knew that." the program is not effective. Desired reactions include:

- "I never thought of it that way."
- "That surprises me!"
- "That's a great idea!"
- "I'd almost forgotten about that...."
- "I can use this."

6.1 Start with a Bang

Experienced, in-demand speakers do not start a presentation with a long, dry, boring introduction that lists every law, regulation, policy, standard, guideline, or other requirement that relates to information security. If there were such a thing as a deadly sin in an awareness

program, it would be to bore the audience. To get an awareness message across, the audience must identify with the idea, concept, or vision.

6.2 Use Logos, Themes and Images

Well-designed security logos and mascots can be a source of pride and a show-piece for the organization. Images have greater impact than words. Color and design, as well as the uniqueness of the image, add to the image's effectiveness. Careful use of animated images in presentations, computer- and web-based courses, and screen savers can enhance the message. A web-based course used by many U.S. Government organizations opens with the words, "What would happen if someone changed your data?" The words are an animated image that changes a few characters at a time until the message becomes completely unreadable: "Wyad ciunx safer ef stmxune khopgel joor deko?" This image makes a dramatic point about data integrity and availability.

Themes can be used to unite several concepts into a related message. The theme of "prevention is better than cure" would be appropriate for organizations that process medical data. Give-away items, such as first-aid kits with security slogans and contact information imprinted on them could tie in to a medical theme, as could the concepts of virus checking software and backups being similar to health insurance cards in that they must be current to be of value.

The U.S. Nuclear Regulatory Agency celebrates International Computer Security Day each year with a different theme. Recent themes included "Keep it clean" where an NRC Computer Security Officer (CSO) dressed as Mr. Clean (complete with a bald head and gold hoop earring) passed out anti-virus software to employees who attended the event. A large, signed color photograph of the official Mr. Clean was on display. Another year, the theme introduced the agency's new security mascot, Cyber Tyger. Cyber Tyger was featured on posters, on the cover of the anti-virus software CD, and on buttons. Again, one of NRC's CSOs arrived in costume and delighted the visitors. Other years the themes have included "It's a Bug's Life" and "PC Doctor" where a "sick" PC was wheeled into the lobby on a Gurney while the CSO, dressed in surgical scrubs and mask, explained the symptoms of a virus infection to visitors.

Awareness posters can be built around a common theme, with common design elements, or a phrase or logo. A staged campaign of posters might include a series with numbers on them, for example, "85" on one and "3 million" on another. No explanation of the numbers would be given and a mystery would develop. Later, new posters could explain that 85 is the number of incidents reported at the organization in the last year and that 3 million is the number of dollars of lost business from a distributed denial of service attack.

6.3 Use Stories and Examples

Stories about real people and real consequences (people being praised, disciplined, or fired) are useful in presentations and courses. Sources of stories include individuals who have been with the organization for a long time and have a "corporate memory," news events, Internet special interest bulletin boards, and security personnel who attend special interest group meetings and conferences.

The stories should relate to situations and decisions the audience will be facing. Stories about hackers accessing medical records would be useful to organizations that process medical data,

while stories about fraud or identity theft would be of interest to personnel involved in the financial industry or the accounting function of an organization.

6.4 Use Failure

Expectation failure is one of the most important learning accelerators there is. Many people do not pay attention to information that is what they are expecting to hear or see. When an employee takes a computer-based awareness quiz and gets an answer wrong, the employee will pay more attention. Failure should be safe and private. For this reason, computer-based awareness questions and quizzes should provide immediate feedback, but should not record answers. At the awareness level, it is more important to give staff something to think about than to allow them to get every answer correct. To remove anxiety, staff members should be informed that their answers are not recorded.

An example of a quiz question designed to engender thought would be:

The building is on fire. As you exit the building in a safe and orderly manner, you are able to take either the data backups or the backup of your custom-built application. Which do you take?

- A. *The data*
- B. *The backup*

Either answer the user chooses is considered correct. The answer screens for each answer tell the user that it does not matter which they picked. The important thing is that they have thought about the possibility of a fire in the building and about making backups. Some users may complain about there not being a single, correct answer; however, more will appreciate the idea behind the question and have a favorable response. In reality, there are times when a person will have to make a difficult choice and often there is not a single right answer.

6.5 Ask Questions and Involve the Audience

Awareness activities that are active and involve the audience are more memorable than passive ones. Whether in person, by poster, or by a web-based awareness course, involving the audience with questions such as “Did you know . . .?” and “What would you do if . . .” is an effective awareness technique.

Trivia questions and unexpected or counter-intuitive facts are good attention getters. For example, asking,

“In the United States, which of the following activities is illegal?”

- A. *Creating a virus that spreads through e-mail,*
- B. *Disrupting Internet communications, or*
- C. *Failing to make daily back ups of data.”*

usually results in people choosing the first answer. The question is designed to be tricky, because creating a virus is not actually illegal. Releasing a virus is, but that is not one of the answers. The correct answer is “Disrupting Internet communications.” The question is designed to get people to think about security in new ways.

6.6 Be Surprising

Well-crafted awareness material is like a piñata; when the audience breaks it open, it should be full of surprises. An activity that often results in wonderful surprises and learning is role playing. Role play (live, or by means of computer- or web-based simulations) is an excellent way to show the target audience what is expected of them. At a recent security educators' conference two educators did an impromptu role play of a worker dealing with a boss who wanted to tail gate, that is to follow the employee through a secure door that had been opened with the employee's cardkey. The audience was entertained and learned by example how to handle such a situation and how to teach others to do the same. Audience members will remember the role play long after they have forgotten the material presented on slides.

6.7 User Acknowledgment and Sign-off

Another technique for getting people to pay attention is to hold them personally responsible for their actions and choices. Many organizations have established policies requiring that an individual's system access be removed if documented awareness orientations or refreshers are not recorded for those individuals by the end of each fiscal year.

"Noisy prosecutions" are an excellent way to discourage security breaches. Organizations may be reluctant to report security incidents out of concerns for losing public confidence. Reporting incidents, however, allows trends to be tracked and may result in faster identification and response to problems.

6.8 Use Analogies

Analogies, metaphors, and similes help learners to associate new concepts with their previous knowledge or experience. These figures of speech create pictures that connect the teacher and learner to the same idea. Famous U.S. trial lawyer, Gerry Spence says, "Words that do not create images should be discarded." Saying that an organization that has a firewall, but does not prevent users from installing modems in their desktop PCs is "like putting a steel door on a straw house" allows readers to visualize the concept.

Analogies can be used to make complex topics simpler to understand. Use analogies to form a bridge between what the learner already knows and the new concept or idea that the learner is expected to understand. For example, a common analogy used to explain password protection techniques is that passwords are like toothbrushes (change them often; never share). Another analogy is that passwords are like bubble gum (strongest when fresh; should be used by an individual, not a group; and if left laying around, will create a sticky mess). A memorable analogy, especially if accompanied by an illustration, would be that passwords are like long underwear, and should be long and mysterious; should protect the owner; should be used by one person, not a group; and should be changed periodically. The more creative or unusual the analogy, the more likely it is to be remembered.

Another analogy is that sensitive data is like prescription medicine: it should be used only by those who need it and who are authorized to have it; it should not be transferred, sold, or given to those for whom it is not authorized; and it can cause damage if it is given to people who do not have a legitimate need for it. Cars, medieval castles, and American Indian and European folklore, among other topics, have been successfully used to present information security concepts.

6.9 Humor

Humor is an effective attention getter and it can be used to motivate people and influence an organization's culture. It also helps people relax, which facilitates learning. Two rules for using humor in awareness presentations, courses, and materials are:

- 1) The humor must be relevant and should complement or augment the message. Humor must be used for a purpose; otherwise it is a distraction and will cause a loss of credibility.
- 2) Do not use humor that will offend your audience. Avoid sexist, ethnic, religious, political, and bathroom humor. Do not make fun of something that cannot be changed, such as a physical or social characteristic (e.g., an extra limb or stuttering).

It is often more acceptable to use humor involving oneself or those in positions of power, such as management and auditors (unless they are a part of the audience). For example, a presenter might say, "The auditor is the one who arrives after the battle and bayonets the wounded" to an audience of managers. Of course, the possibility of backfiring should be carefully considered. A consultant for disaster recovery sites might explain about having a one-page disaster plan: "The plan is simple. It has only two steps: First, I always keep a copy of my resume up-to-date; and second, I store a backup copy in a secure, off-site location."

Sources of humor include:

- Cartoons. For example Dilbert drawn by Scott Adams often deals with organizational and technology humor;
- Humorous definitions. For example "the Arnold Schwarzenegger virus - it'll be back");
- Security-related poems or lyrics written to the tunes of popular songs or in a specific style, such as an information security rap;
- Here is an example of a security haiku, a 17- syllable poem composed in three lines of five, seven, and five syllables:

Computer virus,
destroyer of files, survives
through lack of scanning.

- David Letterman style "top ten" lists, such as the top ten excuses for not making a backup.

6.10 Address Personality and Learning Styles

Trainers often mention three primary learning styles: auditory, visual, and kinesthetic. An auditory learner picks up information from hearing it and is effectively reached by lectures and written material. A predominantly visual learner wants to see what is being taught and prefers diagrams, charts, and pictures. A predominantly kinesthetic learner responds well to tactile input and will want to walk through the steps or learn by physically doing the task.

Personality styles are arguably more important than learning styles. Some people will not follow a procedure until they understand the reason for it. To reach these people, present the whys. If an exercise is included as part of an awareness course, once a question is answered, give learners the choice of trying again or receiving the answer. Some personalities learn best and

have better retention when they figure out something for themselves. Others just want to see the result and move on to the next topic or exercise.

6.11 Take Advantage of Circumstances

Sometimes it takes an outsider, a security breach, or a disaster to focus attention on security. A disaster, such as a fire, can have an invigorating effect and clear the landscape for new growth. Current events can be an excellent source for material and can add credibility to an awareness program. Several Internet security and technology sites offer subscriptions to electronic security alerts and news clippings. Some organizations have established a “news hawk” program, where rewards are given to the first employee to bring a new, relevant story that can be used as part of the awareness program. This is also a good technique to gain “buy-in” from the end user community.

7 Tools

When choosing tools to convey an awareness message, three questions should be addressed:

- What tools are most appropriate for the message?
- What methods are most likely to be credible to and accessible by the target audience?
- Which methods, and how many methods are feasible, considering the budget and the time frame?

Using as many methods and tools as possible continually reinforces the message and increases the likelihood that the audience will be exposed to the message often enough or long enough to absorb it.

7.1 Intranet and/or Internet

Browser-based tools include web sites on the Internet, on the organization’s intranet, and web-based courses. E-mail can be used to send alerts or electronic newsletters (e-zines). Web sites (public or private) can be used:

- as a research tool for gathering information,
- to present policies and other documents,
- to post alerts,
- to collect data on forms, such as for security awareness surveys or incident reporting,
- for self-assessments to identify at-risk security practices,
- for anonymous reporting of security concerns, and
- for web casts of security conferences or presentations.

Web-based awareness courses are useful when the organization has many people who are in several locations and who need to take the refresher or course at a time that is convenient for them. Web-based courses are especially well suited for use by individuals who have diverse backgrounds and experience with technology. On-line courses offer the following advantages over traditional place-based and instructor-led training:

- Feedback is immediate, so learners do not build on early misunderstandings. Well-designed web-based training takes cultural and personality differences into account and reassures timid trainees while allowing more confident ones to progress at a faster pace. “Why” buttons or links, “How” buttons, “Show me an example” buttons, and “Give me an alternative” buttons can be set up to let learners with different needs and personalities use the course to learn in ways that are comfortable for them.
- It’s convenient for the trainees since a web-based awareness course can take place at any time the learner wants. It does not have to be scheduled, so those with variable or hectic schedules can arrange to take the course at a time that is good for them.
- Web-based courses allow users to make mistakes and learn from them in a safe, non-threatening environment.
- Web-based courses are flexible and can be customized to accommodate learners with different levels of experience and different interests. By placing detailed information in subordinate, linked pages, users are able to choose between the “need to know” main pages, and the “nice to know” hyperlinked pages.
- Web-based courses can reduce costs and training time. Updates to courses on the web eliminate the work involved with distributing the current version and materials to many locations. This can be more efficient and consistent because the content has been reviewed, edited, and tested to make it clear and concise.

Exciting and effective web-based courses should:

- Start with a bang - a story, an image, a headline, or something that immediately engages the learner’s attention. Courses should never start with a dull, “why you need this training. . .” introduction. Writer Paul O’Neil offers some excellent advice to writers that applies to creators of awareness programs: “Always grab the reader by the throat in the first paragraph, sink your thumbs into his windpipe in the second, and hold him against the wall until the tag line.”
- Be goal-based, allowing learners to choose how and when they will meet the course requirements.
- Be active and involve learning by doing.
- Address multiple learning styles and personalities. Appealing to multiple senses increases retention. Appealing to different personality styles ensures that the message will reach a wider audience.
- Challenge the learner’s beliefs and expectations and allow learners to fail in interesting and safe ways.

- Use examples and analogies - people learn best from reality and situations where they can relate the learning to prior knowledge.
- Provide feedback, such as immediate answers to questions - feedback is essential to motivation and performance.
- Be memorable. People tend to remember things that are unusual, unexpected, or that carry a visceral impact. Repetition also contributes to how memorable an idea is.
- Include stories. Stories grab people's attention. Organizations should collect stories about security incidents, security heroes, mistakes made, and lessons learned.
- Be accessible. Guidelines for creating web pages that are accessible to people with vision or hearing impairments are published by the World Wide Web Consortium (W3C). To be accessible, the web pages should not rely on vision or sound alone to impart meaning. For example, all graphics should be labeled with text that explains what the graphic is and the contrast between the text and the background should be maximized. An alternative would be to create and maintain two versions of an on-line course.

Well-designed web-based courses meet the above criteria. A potential problem to be alert for is that some developers have a tendency to get carried away by the technology. Just because an awareness course could have three dozen animated, singing computers decorating the pages, does not mean that it should. The technology must be used appropriately; bigger buildings do not make better scholars, and more impressive technology does not necessarily result in a better learning experience. A web-based course that is overloaded with animations and graphics that do not relate to course content, or that has a poorly-designed user interface, will set the awareness program back.

7.2 Screen Savers

Screen savers are a graphic form of communication and like posters, should be eye-catching. Involving a professional artist will help get the message across effectively. Screen savers should contain contact information for the organization's security and incident handling functions. Animations or trivia and questions and answers may make the screen saver more interesting. Screen savers should be updated periodically to keep the message fresh. Commercially produced security screen savers are available with enterprise-wide licensing for entire organizations.

7.3 Sign-on Screen Messages

With some systems, it is possible to add a text message to the log-on or sign-on screen. As with other awareness messages, these should be short, to the point, and frequently changed.

7.4 Posters

A poster series with themes or related designs can be used to highlight specific security issues. Posters should be colorful and should present a single message or idea. Using a professional artist (in-house or external) to design the posters will increase the poster's impact. Posters should be larger than standard letter size to stand out and gain attention. Posters should be changed or rotated regularly and placed at eye-level in many locations. Posters can be printed on both sides of the paper, saving paper and shipping costs for organizations with multiple locations.

7.5 Videos

Videos can be formatted for VHS tapes and digitally on CD-ROMs. Videos can be used at orientation briefings and "brown bag" lunches for staff. Popcorn can be provided in bags pre-printed with security messages. Videos are useful as starting points for discussions and for briefings. Most security awareness videos are less than 20 minutes long. Advantages of videos include that they provide a consistent message throughout the organization and can be provided to staff at distributed locations, saving instructor travel time and costs. Security awareness videos are available commercially from several vendors, and many videos have been produced by the U.S. Government and are available at no charge. Videos can be expensive to produce, with costs averaging \$3,000 per finished minute. Also, as rapidly as technology and threats change, videos can become out-of-date rather quickly. An option is to produce an awareness video in digital format that is designed in segments to allow for updates to portions as the environment or organizational needs change.

7.6 Trinkets and Give-aways

Various give away items can be imprinted with a security slogan and contact information, such as security staff phone numbers or the organization's security web site address. Examples of give-away items are:

- Pencils, pens, high-lighters – "report security breeches – it's the 'write' thing to do"
- Erasers – "wipe out password sharing"
- Notepads – "note who should be in your area and challenge strangers"
- Frisbees – "our information security program is taking off"
- Mouse pads and inserts – the mouse pads have a clear cover over an area into which removable paper inserts are placed; making the cost to change the message far less than the cost of printing new mouse pads
- Key chains – "you are the key to information security"
- Flashlights – "keep the spot light on security"
- Cups or mugs – "Awareness - the best part of SecuriTEA" (where the campaign has explained that TEA stands for training, education, and awareness)
- Magnets, buttons, stickers – "stick with security"
- First-aid kits – "be prepared for security"
- Rulers, calculators – "security counts"

- Coasters, toys, hand exercisers, informational cards, and other items including posters, virus scanning software, and screen savers.

Larger, more expensive items such as T-shirts, tote bags, and gift certificates can be used as prizes for raffles at security events. The more useful, beautiful, or cleverly designed the item, the greater the likelihood that it will be kept.

7.7 Publications

Publications, such as newsletters and magazines, in paper or electronically formatted e-zines, may be devoted to security or may contain articles on security-related events or items of interest. Memos and alerts concerning security issues can be distributed to staff. To get attention, consider stapling a Kleenex™ tissue to stressful memos, such as ones that may be perceived as adding inconvenience or an additional burden on users. Brochures, pamphlets, and comic books can be targeted to specific audiences.

7.8 Surveys, Suggestion Programs, and Contests with Prizes and Awards

Surveys, suggestion programs, and contests help to achieve buy-in. Contests to suggest or name a security mascot, to provide poster ideas, or even suggestions for improving security can boost morale and contribute to team spirit. At presentations, speakers can tape prizes or awards under seats in the front row to encourage people to come early and sit up front.

7.9 Inspections and Audits

Inspections and audits raise awareness among the staff being reviewed, at least for the duration of the inspection. Another technique, called “SBWA” for Security By Wandering Around, involves catching staff members doing something right. If no audits are scheduled, a security staff member can tour the work area at the end of the day and leave certificates of congratulations, thank you notes, or trinkets on the desks of people who have locked all sensitive information in cabinets before leaving to provide motivation. Randomness in such activities is more effective than regularly scheduled inspections. Another possibility would be to have the security personnel periodically demonstrate social engineering by attempting to smooth talk users into giving out their passwords. Users who refuse would be rewarded and users who fall for the scheme would be instructed that they have failed a random security test and will be tested again sometime within the next six months.

7.10 Events, Conferences, Briefings, and Presentations

Participation in events such as International Computer Security Day, on November 30 each year, or in any of the various information security conferences raises awareness. Other events that can contribute to awareness include:

- A “Grill Your Security Officer Cook-Out” where food is served and staff are encouraged to bring any questions about security to the security officer.
- Lectures by dynamic speakers. A boring speaker will hurt the program’s credibility, but a talented professional speaker can be eye-opening. Sometimes, personnel are more accepting of information presented by an independent subject matter expert. Some organizations sponsor a monthly lecture series or lunch presentation on relevant topics.

- Security awareness briefings. Briefings are typically given to senior executives who have little time to spare and to new arrivals who need an overview of the organization's information security awareness policy prior to being granted system access.

8 Measurement and Evaluation

The price security personnel pay for management support includes measurement. Measurement should include the number of people who received awareness orientations and refreshers. This can be determined through attendance sheets, course registrations or completion notifications for on-line courses, and signed user "acceptance of responsibilities" statements.

As with training, an awareness program that does not reach the intended audience is expensive, even if the per capita cost is low. To assess the effects of an awareness program, several measurements and methods may be used. Empirical evidence such as feedback from presenters, audiences, and supervisors is one of the most useful sources of measurement information. Aspects of the awareness program that can be measured include:

- Audience satisfaction;
- Learning or teaching effectiveness; and
- Skill transfer.

8.1 Audience Satisfaction

Audience satisfaction can be measured after-the-fact with course or presentation evaluations or surveys about the awareness program. "Smiley face" evaluations, where the audience is asked to rate the program or activity on a scale, measure how well the audience liked the course, activity, or materials. User feedback may be requested on the presentation's relevance and effectiveness. Asking for suggestions is also a good approach.

8.2 Learning or Teaching Effectiveness

Pre- and post-tests are useful in determining what the audience remembered, and therefore, in tailoring more effective future programs. Unless a pre-program test or preliminary survey is conducted, measuring improvement is virtually impossible.

8.3 Skill Transfer or Audience Performance

This type of evaluation goes beyond the learner to gather input from an outside evaluator, such as a supervisor, security practitioner, incident response teams, or help desk personnel. Follow-up interviews, walk-through testing, help desk and incident reporting statistics, and audit findings can be used to measure improvements in awareness and job performance. For example, prior to an awareness campaign on password construction and management, a password-cracking program could be run to identify passwords that are subject to guessing or compromise. The same program could be run after the awareness activities, and the results compared. Or, an evaluator could walk through the work areas at lunch time testing for terminals that are unattended but not logged off. The same inspection could be performed at various times after the awareness program is initiated. Similarly, a survey of attitudes and specific

knowledge could be taken prior to awareness efforts. Staff might be asked to whom they should report an incident or if they may take older versions of upgraded software home for use once newer versions have been licensed by the organization. Similar questions would be asked at intervals after the awareness program is implemented and the results compared. Another measure is to monitor the number and type of incidents, realizing that an initial increase in reported incidents may be a sign that the awareness program is working and should not be considered negative.

Regardless of the specific measurement taken, a baseline is needed and data for the baseline should be gathered before the awareness program is implemented.

As with any awareness campaign, a security awareness effort will require repetition from year to year to achieve and maintain the desired impact on or changes in behavior.

9 Resources

The Federal Information System Security Educators' Association (FISSEA) produces a newsletter, manages a member e-mail list, and presents an annual conference. FISSEA is a part of the National Institute of Standards and Technology (NIST); for more information, see

<http://csrs.nist.gov/organizations/fissea.html>

Among other documents, NIST is responsible for NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model." This document contains a chapter focused on evaluating training effectiveness; see <http://csrs.nist.gov/training/800-16.pdf> for the document.

The Computer Security Institute produces a Buyer's Guide that lists products and vendors. The Buyer's Guide has a category for awareness materials; for more information see:

<http://www.gocsi.com>

Educational Information Security Materials specifically for children are available from:

The Computer Learning Foundation, <http://www.computerlearning.org/>
The Atterbury Foundation, <http://www.atterbury.org>

Information Security Videos are available from the following vendors:

Commonwealth Films, Inc.
info@commonwealthfilms.com
<http://www.commonwealthfilms.com>
(617) 262-5634

Software & Information Industry Association (formerly, Software Publishers Association)
<http://www.siiia.net>

Notes:

¹ Computer World, "How To Spend a Dollar on Security," Patrick McBride, November 9, 2000.

² Within 60 days is the requirement for U.S. federal employees per Office of Personnel Management (OPM) regulation: 5 CFR Part 930, RIN 3205-AD43.

³ "Practices for Securing Critical Information Assets," January 2000 by the Critical Infrastructure Assurance Office (Chapter 1, page 5).