1-06-35 Establishing a Security Awareness Program

Mark Desman

Payoff

Organizations must regularly inform all users about information security requirements and allocate resources to build and maintain a security awareness program. This article discusses several ways to disseminate security guidelines throughout the organization in a cost-effective manner. Such issues as how to take advantage of existing resources and how to train new employees are discussed. Tips on how to measure the effectiveness of the program and enhance its impact are also included.

Problems Addressed

Protection of information is not an IS issue but a corporate responsibility. Federal and state regulators and legislatures are taking a greater interest in regulating the availability and distribution of information and in securing information against deliberate misuse, theft, or damage. Currently, no regulation addresses the information storage medium. Because the actions of corporate personnel can potentially be very damaging, personnel should be informed of the constraints established by law and by standard security practices and should understand the reasons for their establishment.

The purpose of a security awareness program is to explain to personnel the importance of the information they handle and the legal and business reasons for maintaining its confidentiality. Employees must understand their responsibilities and the steps the organization will take to ensure security.

The Goals of a Security Awareness Program

A security awareness program should be tailored to the organization. It should focus primarily on security issues common to most or all employees. A security awareness program should cover:

- What information should be protected.
- Security measures employees can take.
- What employees should do if a problem is found.

What Information Should Be Protected

The information that needs protection varies from organization to organization. For example, bank and insurance company employees must understand customer privacy issues, manufacturers must protect trade secrets, and oil companies must secure information about explorations. Every organization must protect employee information (especially payroll data), long-term business and marketing strategies, and supply and inventory information.
Devising a Classification System.

Classifying information according to different security levels, a method used by the military, has been adopted by some businesses to alert employees to sensitive information. Clearly labeling a report, tape, or diskette to identify the sensitivity of the contents is extremely effective. A classification label also alerts employees that information requires special handling during distribution, storage, and disposal. Mail clerks, for example, cannot provide special handling for sensitive documents unless they know which envelopes contain sensitive materials. Guidelines for handling different security classifications should be clearly presented to employees.

Reports can be classified in many ways, the simplest of which is to label a report's cover sheet as classified before the report is distributed. Beyond that, programming changes to classify each document page is relatively simple. With this form of classification system, each document handler receives a classification message even when the document is broken up for distribution. This method is also used to notify users of a report's sensitivity at each of the report's iterations.

Security Measures Employees Can Take

Management should remember that what seems obvious to a security expert may not be obvious to another employee. Because employees are more likely to conform to security guidelines when they understand the reasons behind them, the importance of controls should be reinforced by examples. For example, a bank wire-transfer fraud can be used to illustrate what can happen when password secrecy is compromised. It is important to emphasize the practical steps that each employee should follow to promote security in both routine and emergency situations. The general topics and the specific control measures that should be explained to employees in a security awareness program are:

- **Password management.** Procedures for password selection and change, rules against sharing passwords, and the password holder's accountability for its use.

- **Physical access controls.** Keeping keys under control, not allowing piggybacking into restricted areas, escorting visitors, and wearing badges.

- **Environmental controls.** Fire prevention and suppression and use of plastic sheeting to protect equipment from water leaks.

- **Information storage.** Locking up sensitive information when not in use and protecting essential information from destruction.

- **Information distribution.** Packaging sensitive information for mailing, using special messengers or couriers, and verifying caller identity before revealing information over the telephone.

- **Information disposal.** Shredder location and use, using special locked containers for sensitive information, and enforcing a classified-waste disposal program.

- **Authorization.** Knowing who should authorize transactions and when, and the importance of verifying authorization signatures.
· **Errors.** Error prevention, detection, and correction; use of balancing reports or control totals; and actions to take if an error cannot be corrected using standard procedures.

· **Personal conduct.** The importance of not discussing controlled information or the methods used to control it.

· **Disaster recovery.** Each employee's responsibilities in an emergency; knowing who is in charge of special recovery teams and their responsibilities.

· **Personal computing.** Treating information on a desktop computer with the same degree of care given to information on a mainframe.

**What Employees Should Do If a Problem Is Found**

Alert employees who understand the need for security and the principles behind controls can help detect internal fraud and other security problems if they know what to look for and what action to take. Although management must avoid creating an environment in which every employee feels watched, it must ensure that employees do not ignore problems simply because they do not know how to respond. This is especially important if an employee feels that a supervisor may be part of the problem.

**Reporting Security Problems.**

Each employee should know who is responsible for security investigations and should understand the role of internal auditors, data security personnel, and anyone else involved in investigating a security problem. In many organizations, employees report security problems to a designated representative (who must be able to distinguish between true security threats, false alarms, and the actions of disgruntled employees trying to make trouble for their supervisors or colleagues). The telephone numbers of the company's security guards should be published. Everyone should know to whom to report a fire or a suspicious person lurking outside the building. The telephone list should also include the number to call in a medical emergency.

**Employees Can Improve the System.**

An employee who understands the need for security may devise a way to improve controls. Employee suggestions for evaluating and improving the system can be very useful. Anyone discovering a new or better way to control information should receive recognition or a reward from management. Publicizing an employee's suggestions can encourage others to offer ideas.

The most effective means of encouraging employees to identify problems, however, is to explain the risk of letting the situation go uncorrected. Awareness publications must stress that the employee's personal gain and loss relates directly to the company's welfare.

**A Word of Caution**

Thorough employee security education should not include detailed instructions on how to commit fraud. Mentioning that a company lost money to someone who found important information in the trash is sufficient to stress the need for control; a detailed description of how that information was used is unnecessary. A manufacturer of silicon chips can
emphasize the impact of product theft on the company without divulging how much a
cOMPetitor would pay to obtain those chips. An insurance company can stress the
importance of accurately posting premium payments without discussing ways in which the
payment processing system could be used for embezzlement. In other words, training
should be general enough to make the point without suggesting how an employee could
profit from a security weakness.

Management should never cite an example from the company's history. Although such
an example would certainly convince employees that it can indeed happen here, it could
also encourage someone to try the same tactic. Citing an example might also inadvertently
disclose information never reported to the police or the media, which could embarrass the
company and damage its security program.

Understanding the Business Environment

To effectively address information security, the IS management team must be aware of the
background of the organization's employees. Despite increased computer literacy in the
business world, the audience is primarily nontechnical. Presentation materials must reflect
this, and an effort should be made to avoid technical jargon to reach a greater percentage of
the audience. If acronyms or jargon are used, they should be explained fully. Effective
interactive communication can often create a stronger message, because the trainee will
usually appreciate access to a technical resource.

It is important for the IS team to understand the job functions of each security trainee.
A working understanding of user departments aids in clarifying and directing the security
program. A general knowledge of the business also aids in creating a security program that
meets the needs of the corporation, does not inhibit work, and provides sufficient levels of
integrity.

IS management should evaluate the existing security system and awareness program
before structuring a new program. Although it may seem easier or more desirable to
initiate a new program, that is rarely the case. Improving an existing program is usually
more effective. If substantial deficiencies exist, they must be corrected before
implementing an awareness program.

For a user awareness program to be successful, a practical and demonstrable security
program must back it. For example, the IS staff must verify that access controls are in
place and are well documented. Complete and accurate documentation is basic to any
awareness program, and the program's policies must be traceable to standards, policies,
and procedures currently in place.

Identifying the data owners for each system is another important aspect of
implementing an awareness program. Because the data owner defines how access is to be
granted, the concept of ownership places responsibility at a high enough level within the
organization to ensure that conformance to security procedures is enforceable.

The Effects of Distributed Processing

The proliferation of microcomputers raises the issue of protecting company
information and software entrusted to system users. This can be complicated because it
involves the protection not of a centralized computer system that can be monitored from a
single point but of a widely scattered group of processors and users. IS management must
therefore establish policies for the use of such equipment and a means to review
compliance. Again, self-policing is the most effective means to gain users’ cooperation.
The availability of shareware and computer bulletin boards has fostered the spread of computer viruses across networked systems. The IS department can combat this problem by distributing a bulletin or newsletter stating the company policy against the use of nonapproved software and informing users how to detect, prevent, and report viruses. Several different virus detection and removal products are on the market; at least one should be available in any company that uses microcomputers.

Because of the relative ease with which users can make unauthorized copies of microcomputer software, software producers have formed a coalition called the Software Publishers Association (SPA). The organization has won sizable settlements against many well-known companies for misuse of its members’ products. The Software Publishers Association has even established an 800 number for reporting suspected instances of software piracy. Organizations must therefore keep strict inventory of their purchased software. Policy statements regarding the introduction of nonapproved software or second copies of legitimately purchased software must be communicated when microcomputers and associated software are installed. Periodic inventories not only safeguard against litigation but regularly remind users of the importance of using only legitimate copies of purchased software. (Programs are available that can identify hard disk-resident products.) An inventory sheet should also accompany each microcomputer, listing the programs that can legitimately be used on it.

Perhaps the best means for controlling the use of microcomputers and increasing security awareness is to establish a microcomputer center that assumes responsibility for ordering hardware and software as well as training and reviewing new technology. It would also maintain copies of inventory and virus detection programs and could produce a security-oriented newsletter for microcomputer users.

**The Corporate Security Policy**

Communicating a corporate viewpoint on information security requires defining what is being done and why. An outline of a planned awareness program should be presented to corporate managers to make them aware of the proposed program, to define the reasons for the program’s creation, and to gain approval. Later, when program documentation is prepared for general distribution and employee-orientation presentations are established, management's support should be evident.

The initial step in implementing a security awareness program is to obtain from corporate management a clear statement of the company's policy on the value of information and security. This information security policy is now expected to be in place in all corporations and is well worth the time necessary to obtain it. This policy document is simple and straightforward: a single-page document indicating the company's view of information as a company asset and its exact expectations of employees. It is critical that this viewpoint be explicit and that the company's willingness to take action against misusers be clearly stated. The policy should also be submitted to the company's board of directors for its approval and should be published in whatever policy and procedure manuals are used in the organization. It should be distributed throughout the company and included in a security presentation for orienting new employees.

**Security Training Methods**

Teaching usually connotes lecturing to a group of people and then answering questions. A company that employs more than several hundred people, however, is probably too large
for this method. The following sections discuss less time-consuming methods that can deliver a security message more effectively.

**Employee Orientation**

The formal employee orientation program provides an ideal opportunity to introduce the concepts of information security and data handling. The security awareness presentation should be brief, but it should inform all new employees of the company's expectations. Employees will perceive the company's general attitude toward security as part of the corporate culture. Human resources departments can often help with orientation materials, thus absorbing some of the cost for security training.

If possible, handout materials should include a formal pamphlet featuring the corporate security policy and an overview of the programs in effect. A summary of access controls, log-on ID and password standards, and prepared responses to often-asked questions should also be included. This material is usually presented in greater detail in standards manuals, but employees may not encounter them later on.

Another document that must be available for the orientation program is the security statement form. This single-page form contains a series of statements regarding how an employee should act under given circumstances (see Exhibit 1). This is the employee's agreement to abide by the rules and is acknowledged by a signature. The original copy of the form can be kept in the employee's personnel file. This agreement can be reinforced periodically by presenting it for signature again. Current employees should be presented the same form.

**Sample Information Security Statement**
It is the policy of this company to view information as a corporate asset. Misuse or damage of information may be as costly to the company as would similar action on physical property. Your own responsibility for protection of company information is outlined below. Please read it carefully before signing.

1. I will use company information and third-party proprietary information only for the performance of company business.
2. I will not alter or in any way change company information except in the performance of the duties of my job.
3. I will not divulge company or third-party information to anyone whose relationship with the company as an employee, customer, or contracted temporary employee does not warrant it.
4. I will not attempt to gain access to information or facilities to which I am not specifically authorized.
5. I will use the data processing facilities of the company only in a manner consistent with my job function and for conducting company business.
6. I will not maintain personal information, information for businesses other than the company's, or any form of noncompany data on company computer equipment.
7. I am aware that any user IDs or passwords assigned to me are to be used only by me and are not to be divulged to any other party.
8. I will comply with all company procedures in the assignment and format of my passwords.
9. I am aware that failure to comply with any of the conditions noted herein may result in my being disciplined or terminated from my position. I am also aware that the company retains the right to pursue prosecution when misuse of its information and computing resources is suspected. I have read all of the above conditions and understand them fully.

NAME:___________________________________________________________________
SIGNATURE:______________________________________DATE:___________________
============================================================================

This exercise delineates the individual's personal responsibilities and demonstrates the company's commitment to information security. It also protects against potential litigation regarding security breaches and internal regulations. This document should be presented to the corporate legal department for its review before it is put into effect.

Security Articles and Publications

Members of the IS staff can write a series of articles for the company newsletter covering basic information security concepts, including examples of other organizations' security mishaps and explanations of how they could have been prevented. Articles must be simple and clear. Someone who knows little or nothing about security or controls should be asked to read and comment on the articles to ensure that they are clearly written. Articles should always end with a list of actions that each reader can implement.

A general security booklet is another means of publicizing the security program. Detailed standards for certain audiences (e.g., computer programmers) can be published selectively; however, general security measures that affect all employees should be published in a manual. The security booklet may be combined with an emergency response manual to reduce costs and ensure publication of the security material.

If the organization employs many non-English-speaking people and internal material routinely appears in more than one language, a foreign-language version of the security booklet should be published. The human resources department should be able to provide guidance in this matter.
Computer-Based Training for Microcomputers

Several companies offer security-training software for microcomputers; these packages include a training text as well as practice questions and answers. As an alternative, the IS department can develop a computer-based training course tailored to specific company policies. (Tools for developing such courses are available to facilitate this task.) Some microcomputer security training should be required for all microcomputer users, and it should be presented periodically to refresh and reinforce security awareness.

Presentations

Aside from employee orientation sessions, other formal presentations can introduce new systems and procedures. For example, when a fire-extinguishing system is installed in the computer room, data center personnel should be given a presentation detailing the new system's operation. Ideally, the vendor should make such a presentation because the vendor knows the most about the system.

Informal security presentations should also be considered. Some organizations offer lunchtime lectures on a variety of subjects; security topics could occasionally be recommended. Because attendance at such lectures is voluntary, the presentations must be entertaining as well as informative.

New Systems

When a new computer system is introduced, employees who will be working with it should be instructed in its security controls. For example, each user of a new Electronic Funds Transfer system must be instructed on the use and control of test keys. If a new accounting system depends on certain control totals to detect erroneous or fraudulent data, those responsible for balancing the totals must be aware of the importance of the controls and what steps must be taken if an out-of-balance condition is detected.

The system-user guide must clearly explain the controls and procedures to be used in protecting the system. As with other training material, the instructions must be general enough so that employees cannot learn how to circumvent the controls.

All employees who are issued user IDs and passwords should sign an acknowledgment stating that they have received the password, will use it only for its intended purpose, and will promptly report any suspicions that the password has been compromised. This should be an ongoing procedure for new users of the system as well as for the original users.

Often, certain information must be distributed instantly. A bulletin system is useful for such cases. The use of special bulletins can create an air of urgency about subjects that are time dependent(e.g., new procedures or specific problem areas) and that are closely associated with the data security function. A bulletin template easily produced on a microcomputer can create handouts that promote information security.

Maintaining Security Awareness

All training tends to be forgotten over time. Most people eventually relax some of their diligence in following procedures, particularly those not essential to their jobs. If employees are under pressure to perform at a high level of productivity, they may begin to perceive security controls as a time-consuming impediment and bypass them.
Consequently, the security awareness program must be ongoing to remind employees of their part in the company's security program.

The organization's newsletter is one of the best vehicles for distributing news about information security and for updating procedures. In addition, notices or posters reminding employees of security requirements should be placed in areas in which sensitive information is handled. A poster will, however, lose its effect over time. Leaving the same materials on a bulletin board also dilutes the effect of the message and eventually renders it useless. Ideally, messages should be changed monthly.

**Ensuring Compliance**

Some organizations require their officers or managers to sign an annual acknowledgment or statement that they have reread the policies. This can be extended to other employees, especially those who work in sensitive areas.

Performance appraisals can include an assessment of how well an employee has maintained security. Managers of employees in sensitive jobs should take the opportunity to discuss security procedures and controls at the employee's review and evaluate how well the employee has complied with them. When appropriate, objectives related to security should be included in the goals for the next performance appraisal. However, employees can be fairly rated on compliance with security practices only if they have been informed of such practices. Therefore, this rating factor should be used only in the context of an effectively implemented security awareness program.

**Reviewing the Effectiveness of the Program**

Once a security awareness program is in place, some means must be established to measure its effectiveness and to identify areas where further effort is needed. The internal audit, human resources, and IS departments' review of access violations are the best sources of information. Through constant review, the program can be maintained and upgraded to meet new issues as they develop.

Statistics on security performance are kept by most systems. For example, in an IBM environment, System Management Facility records keep track of most security software products. Items such as automated log-offs can easily be checked to see whether employees log off when leaving a terminal. Those records that are used by the security software packages can be analyzed to identify the number and types of violations. Over a long period—for example, one year from the inception of the new program—trends should be apparent. These records document the effectiveness of the program and indicate where greater emphasis should be directed. Often, patterns will suggest a need for better training within a particular scope of activity.

There are occasions when disciplinary action is warranted. For such action to be carried out, malfeasances must be defined. This is usually a matter of enforcing internal policies and procedures rather than civil law. By working closely with the human resources department, IS management can identify the type of information needed to enforce discipline. The IS department's success in informing employees of their responsibilities will be reflected in a lower number of security breaches.

In cases in which termination or persecution is necessary, the company position regarding the law is of the utmost importance. Because the level of detail in internal educational publications may well determine the success of the action, it is important to ensure that sufficient documentation exists.
In many industries, the state or federal government establishes regulations by which organizations must abide. The legal department evaluates such regulations and defines the company's actions under the law. IS management should be informed of these directives in order to update current documentation and inform employees of their responsibilities.

Feedback from employee questionnaires can provide insight into what can be done to further enhance the awareness program. The questions included may refer to areas where confusion or misdirection have been noted or specific items on which feedback is desired. The questionnaire should be short, with mostly true/false or multiple-choice questions, and it should contain a final Request For Comments or questions.

Finally, program performance may be reviewed by internal EDP auditors. Their observations can help establish a means of measuring security compliance. In addition, the auditors can assist in the creation of the annual audit schedule to address items of mutual concern. Because an internal audit shares one aim of the IS department—to guarantee the integrity of the company's information assets—it can help determine the direction of the security program and, therefore, the basis for the security awareness program.

**Recommended Course of Action**

Putting safeguards into place is only half the job. IS management must also inform the users of:

- The potential effects on employees of a security breach.
- The importance of information as a company asset.
- The responsibility of each individual user for the integrity and privacy of company information.
- The actions expected of users by corporate management.

A security awareness program is often a low-budget project, requiring careful use of resources outside the IS department. The most effective means to do this is to take advantage of existing resources to reach the greatest number of employees. Those resources might include:

- Packaged security awareness tools for microcomputers. These software tools should be loaded on the microcomputers before they are installed in user areas.
- New employee orientation sessions to present the company position on information security.
- Handouts for new employees, presented in an informal and nontechnical format.
- Senior management statements, videotaped if possible but at minimum available as printed materials to be distributed.
- Internal company publications and security articles.
- Bulletins covering specific security issues, including copies of relevant articles appearing in trade publications.
All audit reports should be used to enhance the information security program and to communicate the issues behind any changes to users. By creating and maintaining an interest in the users’ performance, the IS department can further enhance the security awareness of all personnel.

Author Biographies

Mark Desman

Mark Desman is a senior information security specialist with Tandem Computers, Inc., in Cupertino CA. He has been involved in information security for more than 13 years and has successfully implemented many security awareness programs. He has served as information security officer for financial and manufacturing organizations and has consulted in both information security and contingency planning.

Portions of this article were originally written with Leslie Chalmers.