Establishing a Security Awareness Program

Leslie S. Chalmers

Payoff

Most security breaches are caused by employees acting in ways that undermine security controls. Usually such action is not deliberate. With the widespread use of microcomputers, many security controls are manageable only by the employees themselves. An employee security awareness program can alleviate the problem of employee security breaches by clarifying why security is important and controls are needed. This article presents guidelines for establishing a successful security awareness program and offers tips and techniques for encouraging employees to participate in it.

Problem Addressed

As more and more systems are linked to each other and to the outside world through dial-in and network connections, the risk of hacker attacks increases, usually because employees leave paths wide open to attack. Some systems can be accessed without any passwords; others contain the default user IDs and passwords that come with the system; still others employ user IDs with passwords that hackers can easily guess. Only by educating employees about the risks and their personal responsibility for preventing easy access by outsiders can such attacks be prevented.

In the last decade, the growth in the use of microcomputers has been staggering. In some offices, there are now more computers than there are employees. These computers usually do not have such basic security controls as controls for user identification and authentication. Microcomputers are the unique target of certain types of threats, including attacks by computer viruses. Portable computers are especially vulnerable to theft. In such an environment, the responsibility for protection of systems must rest with the personnel who use them: no central authority can ensure that all systems are secured against theft, destruction of data, and browsing of confidential files. Individual employees must protect their systems if they are to be protected at all.

The data security administrator can increase the success of the organization's security program by educating all employees about their role in making the program work. Management must also be involved in ongoing security education and must hold employees accountable for compliance with security controls. This article discusses the elements of an employee security awareness program that can help ensure that controls are everyone's responsibility and concern.

What Must Be Taught

A security awareness program should be tailored to the organization by focusing on security issues common to most or all employees. Programs for securing a particular area should focus on details that affect only that area. In general, an awareness program should cover:

- What should be protected.
- What employee actions are required.
- What employees should do if a problem is found.
What Should Be Protected

The information that needs protection varies among organizations. For example, bank and insurance companies must be aware of customer privacy issues, manufacturers must protect trade secrets, and oil companies must secure information about new explorations. Every organization must protect employee information (particularly payroll data), long-term business and marketing strategies, and supply and inventory information.

The information in a computer is valuable only if it can be trusted to be accurate. For example, just-in-time ordering requires that information about supplies on hand and their rate of consumption be correct; airline customers expect that reservations will be recorded correctly. It is therefore essential that the integrity of critical information be protected.

Where the company is dependent on computer-based information to perform critical functions, the availability of the information (and the systems which process them) must also be ensured. For example, manufacturers and suppliers would go out of business if their sales orders and accounts receivable records were to be lost.

In summary, information must be protected if:

- Its disclosure could cause harm to an individual.
- Its disclosure could cause embarrassment or loss to the company.
- Its alteration could result in financial loss or incorrect management decisions.
- Its destruction could cause an interruption in critical organizational functions.

Many businesses have adopted the military practice of classifying information according to different security levels to alert employees to sensitive information. Clearly labeling a report, tape, or diskette to identify the sensitivity of the contents is very effective. A classification label also alerts the employee that the information requires special handling during distribution, storage, and disposal. For example, mail clerks cannot provide special handling for sensitive documents unless they know which envelopes contain sensitive materials.

It is important that any labeling program be coupled with instructions on the proper handling of the labeled material. Labeled material that is not protected is even more vulnerable to misuse and loss than it would be unlabeled.

What Employee Actions Are Required

Employees are more likely to follow instructions regarding security precautions when they understand the reasons behind them. Consequently, the importance of controls should be reinforced by presenting situations they can relate to; users can quickly understand data vulnerabilities if they realize that there is a personal risk involved. For example, most microcomputer users appreciate the impact that the destruction of their hard disks would have on them.

Although the topics to be covered in a security awareness program vary among organizations, the general topics listed in Exhibit 1 should be included. Employees who use microcomputers should also be trained on the topics listed in Exhibit 2. It is important to emphasize the practical steps that each employee should follow to promote security in both daily routine and emergency situations.

General Security Program Topics
<table>
<thead>
<tr>
<th>Topic</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password management</td>
<td>Procedures for password selection and change, rules against sharing passwords, password holder's accountability for its use</td>
</tr>
<tr>
<td>Physical access controls</td>
<td>Keeping keys under control, not allowing piggy-backing into restricted areas, escorting visitors, wearing badges</td>
</tr>
<tr>
<td>Environmental controls</td>
<td>Fire prevention and suppression, use of plastic sheeting to protect equipment from water leaks</td>
</tr>
<tr>
<td>Information storage</td>
<td>Locking up sensitive information when not in use, protecting essential information from destruction</td>
</tr>
<tr>
<td>Information distribution</td>
<td>Packaging sensitive information for mailing, using special messengers or couriers, verifying caller identity before revealing information over the telephone</td>
</tr>
<tr>
<td>Information disposal</td>
<td>Shredder location and use, using special locked containers for sensitive trash, enforcing classified-waste disposal program</td>
</tr>
<tr>
<td>Authorization</td>
<td>Who should authorize transactions and when, the importance of verifying authorization signatures</td>
</tr>
<tr>
<td>Errors</td>
<td>Error prevention, detection, and correction; use of balancing reports or control totals; what to do if an error cannot be corrected using standard procedures</td>
</tr>
<tr>
<td>Personal conduct</td>
<td>The importance of not discussing controlled information or the methods used to control it</td>
</tr>
<tr>
<td>Disaster recovery</td>
<td>Each employee's responsibilities in an emergency, special recovery teams' responsibilities, who is in charge of those teams</td>
</tr>
<tr>
<td>Information classification</td>
<td>Company standards and labels for distinguishing sensitive information from public information (examples are useful in explaining the concept of classification)</td>
</tr>
<tr>
<td>Legal issues</td>
<td>Legal requirements dictating security practices (e.g., how long information must be retained); other legal requirements may apply to specific industries</td>
</tr>
<tr>
<td>Electronic mail</td>
<td>The company's right to read employees' E-mail; prohibition against using E-mail for personal business; concerns regarding the storage and forwarding of E-mail messages by the recipient</td>
</tr>
<tr>
<td>Portable computers</td>
<td>Information that is not permitted to leave the company's premises (if any); instructions for protecting equipment while travelling</td>
</tr>
</tbody>
</table>

**Microcomputer Security Program Topics**
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 action to take. Although creating an environment in which every employee feels watched should be avoided, care must be taken to ensure 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. Employees may hesitate to report the questionable activities of a supervisor if they do not have a clearly defined mechanism for doing so.

Each employee should know who is responsible for security investigations and should understand the role of internal auditors, the data security administrator, 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 and false alarms or 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 loiterer. The telephone list should also include the number to call in a medical emergency.

An employee who understands the need for security may devise a way to improve controls. An employee suggestion system is an excellent vehicle for collecting such ideas. Anyone discovering a new or better way to control information should receive recognition or a reward from management. Publicizing the suggestions of one employee is one way to encourage others to offer ideas.

Awareness Training for Microcomputer Users

An employee with a desktop computer is a one-person data processing shop. If that user does not make backup copies, no one will. If the user does not limit access to
confidential documents, no one will. If the user does not practice version control over his or her own software, no one will. Because of these and other considerations, the training of personal computer users in information security is especially important.

At a minimum, users must be drilled on the importance of making regular backups of files to overcome such problems as accidental modifications to software or data, contamination by viruses, and erroneous formatting of disks containing important data. Beyond this essential topic, there are many more which the information security manager might consider.

Although information security managers may feel that the threat of computer viruses is overblown, users still need to be aware of how to protect against viruses and how to respond if one is detected. The information security manager might capitalize on periodic virus scares to promote a virus prevention program. For example, the appropriate virus scanning software might be sent to all departments along with a memo reminding people of the importance of maintaining a current backup.

Pirated software is another problem common in microcomputer environments. (Although data processing people may have the ability to copy proprietary software written for larger systems, this is almost never done because of the problem of finding another system where the pirated software can be used.) With the explosion in the use of home computers, employees will be tempted to save money by taking software from the office just as they might pencils. Employees should be informed of the company's position with respect to this practice; if it is not too expensive, site licenses might be negotiated that would legitimize the controlled copying of software.

The security of custom-developed software must also be protected. Even spreadsheet formulas need to be properly controlled. If a revenue forecasting summary formula contains an error, management may approve expenditures based on incorrect revenue forecasts. People who engage in such programming activities must understand the need for testing their code and protecting the tested version from being modified without proper retesting.

The effectiveness of microcomputer user training depends, in part, on the adequacy of the overall training program. (For example, some users who have been advised to "make copies" of their disks for backup purposes have responded by photocopying their diskettes! These users did not know about backup commands and so they copied the only way they knew how.) The information security manager must determine what supplementary training is required to bring users to a level where they can understand the security curriculum, without becoming, in the process, the personal computer trainer for the entire company. Any deficiencies in the overall training program should be brought to the attention of management so the responsible unit can take corrective action.

If a general training program exists, the security manager should also attempt to get security issues included as part of the basic curriculum. Security should be seen to be an integral part of information processing, regardless of the size of the computer.

**Pitfalls to Avoid in Security Training**

Thorough employee security education does not include detailed instructions on how to commit a fraud. Mentioning that a company could lose 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 could be used is unnecessary. A manufacturer can emphasize the impact of product theft on the company without divulging how much a competitor would pay to obtain the product. An insurance company can stress the importance of accurate posting of premium payments without discussing ways in which the payment processing system could be used for embezzlement. Training should be general enough to make the point without suggesting how an employee could profit from a security weakness.
One case of a payroll fraud committed by a computer operator clearly illustrates this point. The individual was given security training in which a case was presented on how a computer operator at another company was able to create phony paychecks and cash them. Unfortunately, the instruction included detailed information on how that individual was caught. Using this information, the computer operator was able to devise an improved scheme that allowed him to steal money through fraudulent paychecks and avoid detection for more than two years.

A security principle should not be emphasized by citing a violation from the company's own history. Although such an example would certainly convince employees that a fraud or other violation could indeed occur at their company, it could also encourage someone to try the same ploy. Citing an example might also inadvertently disclose information never reported to the police or the media. If it is subsequently disclosed by the employees receiving the training, even greater embarrassment could result.

Security Training Methods
The following sections discuss some security training methods that can deliver the security message effectively.

Security Articles and Publications
The data security administrator can write a series of articles for the information center or company newsletter covering basic security concepts, including examples of security mishaps and how they could have been prevented. The articles must be simple and clear. Someone who knows little or nothing about data security or controls should be asked to read and comment on the articles to ensure they can be understood by nontechnical employees. The articles should always end with a list of actions that each reader can take to avoid making the same error.

Tying such articles to items in the news can be an effective way of ensuring they are read. If the media have been reporting on hacker activities in recent weeks, an article on how to select secure passwords should be published. An article on how to prevent virus infections is most effective when viruses are getting a lot of attention.

A general security booklet is another means of publicizing the security program. Too often, information security requirements are published only in a management manual that few employees see. Detailed standards for certain audiences can be published selectively; however, general security measures that affect all employees should be published in a manual or booklet that is distributed to all personnel.

With the increased use of microcomputers, a company might consider creating a special security booklet on protecting these systems. All employees need to be aware of how to securely dispose of sensitive trash, microcomputer users also need to know how to securely dispose of a worn diskette that has been used to store sensitive information.

Computer-Based Training
The microcomputer itself can be used as a vehicle for training microcomputer users. Several companies offer security training software for microcomputers that include training text as well as practice questions and answers. As an alternative, the data security administrator can develop a computer-based training course tailored to specific company policies. However acquired, a microcomputer security training program should be mandatory for all users and presented periodically to refresh and reinforce security awareness.

Training can also be performed using a centralized computer, which can be useful for maintaining statistics on who has taken a computer-based course and when the course was
taken. Users could be required to periodically take a quiz on material contained in a course; if they do not pass, they may be required to retake the course, perhaps in a condensed form.

Computer-based training should be designed with the user's convenience in mind. The user should be able to skip over familiar material, provided they can demonstrate their mastery of the topic. The user should be able to stop the course at any point; the system should take the user back to that point when he or she resumes running the program.

**Presentations**

Formal presentations can be useful to introduce new systems and procedures to affected groups. Informal security presentations should also be considered. Some organizations offer lunchtime lectures on a variety of subjects; security topics could occasionally be included. Because attending such lectures is usually voluntary, care should be taken to make them entertaining as well as informative. Films or videotapes are an effective method of holding an audience's attention and can be obtained from vendors. Films should be prescreened to ensure they are appropriate for the intended audience.

**New Employee Training**

Security awareness must be a part of the orientation program for newly hired employees. Each new employee should be required to sign an agreement to abide by the organization's policies and rules. Although some organizations also have their professional staff sign nondisclosure or noncompetition agreements, these do not commit employees to adhering to company security standards. Only a general compliance statement for all employees alerts them to the importance of security policies and standards.

All new employees should receive copies of the general security rules as well as the specific rules that apply to their work area. If the organization has a security booklet, it should be included in the orientation packet along with the company's standard personnel forms and literature. This emphasizes the organization's commitment to security.

**New Systems**

When a new computer system is introduced, its users should be instructed in its security controls; the system user guide must also clearly explain the controls and procedures to be used in protecting the system. As with other training material, all instructions must be general enough so that employees cannot learn how to circumvent the controls.

All employees who are issued user IDs and passwords for a computer system should sign an acknowledgment stating they have received the password and promise to use it only for its intended purpose and to 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. Anyone who is given a new microcomputer should also be given training on its security requirements.

**Maintaining Security Awareness**

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 total security program.
General Reminders

The data security administrator should continue to publish articles in the organization's newsletter. Subjects that have not been covered for more than a year should be reviewed and brought up to date or discussed from a different perspective. For example, if the organization has implemented an access control software package since the last article on password controls was written, the article should be updated. In addition, notices or posters reminding employees of security requirements should be placed in areas where sensitive information is handled.

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

Security Objectives

Performance appraisals can include an assessment of how well an employee has maintained security and a review of security procedures and controls. Sensitive jobs should have a procedures and controls checklist to be discussed at the employee's review. Each point and how well the employee has complied with it should be examined. When appropriate, objectives related to security should be included in the goals for the next performance review period.

Electronic Mail

In organizations in which E-mail is in wide use, E-mail can serve as an effective means of reminding employees of specific security policies and practices. For example, a new security tip could be broadcast every working day during a month designated as computer security awareness month. Messages might include:

- “Never tell anyone your password.”
- “Did you back up your computer files today?”
- “Never take software from strangers.”
- “Protect information as if your job depended on it. It does.”

Computer-Based Training

Computer-based training can be used for periodically updating or reinforcing security training. For example, employees could be required to go through training once a year. (If there is no new material to be taught, users could obtain an exemption from taking the course by passing a short quiz to prove they remember the material.) A centralized system might be used to keep track of which employees have updated their computer “driving license.”

Games and Contests

Some companies have experienced great success with such activities as computer awareness games, contests and fairs. For example, exhibits might be set up near the company cafeteria, with such door prizes as virus scanning software (properly licensed, of course) given away. Other companies use 800 call-in numbers for contests that reach employees in remote locations; employees who call the number for contest information
receive a one or two sentence awareness message as well. If the contest requires several steps (like a scavenger hunt), each step can be described along with a different awareness tip on successive days.

**Management Responsibilities**

Because managers and supervisors are ultimately responsible for security compliance within their departments, all managers should be involved in the security awareness program and should actively promote security awareness among their staffs and enforce procedures and controls. In addition to the general security presentation given at orientation, new employees should receive job-specific security training from their supervisors. Managers should also hold periodic refresher discussions on these controls.

**Management Compliance**

Because even small deviations from security controls can encourage lax security practices, managers must insist on full compliance. If employees in an area with badge-reader-controlled access are occasionally allowed to piggyback others when the manager is present, they will be likely to continue the practice when the manager is absent.

Managers must also realize that they set the example for their employees. If the manager of a data center smokes in a no-smoking area, everyone else will also ignore the signs. If the manager is careful to extinguish a cigarette before entering the room, the employees also will exercise more care.

**Senior Management Role**

Senior management must also play a role in a security awareness program. In addition to encouraging middle and line managers to support the program, senior management must set clear policies regarding enforcement of the security controls. Senior management should also set a clear policy that protects anyone reporting a problem with controls or their enforcement. Employees who report that a control is being ignored or circumvented should be protected from reprisals by supervisors and colleagues and should be allowed to remain anonymous. For example, the employee could report a problem to an employee relations representative, who would forward the information without revealing its source. Employees who desire recognition for reporting problems should receive it.

**Recommended Course of Action**

Employees who understand the need for security and know what they must do to promote it are the best protection against fraud and careless errors. An organizationwide security awareness program can help develop such behavior by educating everyone about the importance of security. Encouraging employees to comply with controls, identify problems, and suggest ways to improve controls will give them a sense of participation and responsibility.

To introduce users to critical security issues and encourage adherence to the organization's ongoing security policies and procedures, the data security administrator should:

- Ensure that the security awareness program covers what should be protected, what employee actions are required, and what employees should do if a problem is discovered.
• Ensure that although the security education program is thorough and comprehensive, it does not provide detailed information on how to commit a fraud.

• Implement effective security training methods, which include:
  • Publishing security-related articles in the company newsletter.
  • Investigating CBT security packages.
  • Conducting formal and informal security presentations.
  • Educating new employees regarding security controls.
  • Ensuring that users are informed of revised security controls when a new system is introduced.

Maintain security awareness. Keep senior management involved.

Author Biographies

Leslie S. Chalmers
Leslie S. Chalmers is a vice-president of The Bank of California, San Francisco.