

DOES YOUR INSTITUTION ACHIEVE AN "ATMOSPHERE OF SECURITY"?

The FFIEC Information Security Booklet states that "employees should know and be held accountable for fulfilling their security responsibilities." It goes on to say that institutions should ensure that knowledge can be achieved through training, certifications of compliance, self-assessments, audits, and monitoring. It has been Compushare's experience that the majority of financial institutions fall short of effective security awareness.

Any security professional will tell you that the weakest link in security is always people. Even in the movies, how do the spy characters always gain access to secure computer systems? By taking advantage of a person with trusted access, they gain physical access to secure areas.

In order for all of the technical security controls that institutions put in place to be effective, an "Atmosphere of Security" must be created. This atmosphere of security is created through raising the awareness level of all employees and through the direction and example of senior management. We cannot emphasize enough, the importance of senior management buy-in and involvement in establishing an atmosphere or corporate culture where security is second nature to all employees.

In many of the institutions for which we perform security assessments, lack of buy-in by senior management is evident through the setup of their user accounts. More often than not, the President, CEO, and other senior managers are found to have special access privileges that include never having to change their passwords. On top of that, their passwords are among

the worst in complexity, making them easily cracked by simple dictionary methods.

How can employees be expected to follow security policies and practices when it is well known that the top managers do not follow those same policies and practices? Corporate culture is created through the actions and attitudes of the organization's managers. Therefore, the first step in creating an atmosphere of security is for senior management to adhere to the same policies as everyone else.

Most institutions seem to meet the minimum annual certification of compliance where typically, the HR Department makes everyone read the employee related security policies and acknowledge in writing that they have done so. In addition, most institutions perform some sort of annual security training sessions. Where most institutions fall short, is in the area of raising overall awareness.

Institutions that have a dedicated Information Security Officer (ISO) with proper authority levels have achieved far greater success in establishing an atmosphere of security. This is because senior management's commitment to security is passed through the ISO to the departments and employees. The ISO should take charge of security awareness and training.

Many institutions make the mistake of combining awareness and training simply calling it security awareness training. Awareness is not training. Awareness is an ongoing process designed to focus employees' attention on security. Awareness presentations are intended to make

individuals recognize information security concerns and respond accordingly.

Training, on the other hand, is more formal and would have the goal of building knowledge and skills in the mechanisms of security control. A good example for the use of training in financial institutions would be to train managers how to review audit logs and what to look for with respect to potential violations.

A good example of security awareness would be to send a short attention getting email about passwords. The following example is from an awareness campaign at the University of Michigan.

Passwords are like Underwear...

Passwords are like Underwear...

Change yours often.

Passwords are like Underwear...

Don't leave yours lying around.

Passwords are like Underwear...

Don't share them with friends.

Passwords are like Underwear...

Be mysterious.

Passwords are like Underwear...

The longer, the better.

**ITCS at University of Michigan*

The comparison of passwords to underwear uses humor to keep the attention of the reader long enough to get the point across. Employees will remember this humorous comparison because their first thought will be to add a few of their own comparisons to the list. When

they do that, it will help them internalize the information.

According to NIST SP800-16, effective IT security awareness presentations must be designed with the understanding that people develop a tuning-out process known as acclimation. If the same method of providing information is continually used, no matter how stimulating it is, the recipient will selectively ignore the stimulus. Therefore, awareness presentations must be ongoing, creative, and motivational. Awareness presentations should focus employees' attention so that the information provided will be incorporated into conscious decision making. This process where an individual incorporates new experiences into existing behavior patterns is called assimilation.

Learning attained through a single awareness activity will tend to be short-term, immediate, and specific. Repeated awareness activities spread over time improves assimilation. In other words, security awareness training performed once a year will not be assimilated into the existing behavior patterns of individuals. Information Security Officers must develop a program of ongoing security awareness in order to build an atmosphere of security.

Some key topics that should be part of financial institution's security awareness program are as follows:

- Creating secure passwords
- Handling suspicious phone calls
- Challenging unknown persons
- Understanding security related events
- Understanding employee security responsibilities
- Understanding the correct response to certain security events
- Recognizing suspicious PC behavior
- Understanding customer private information

- Understanding the importance of not leaving sensitive information on desks
- Understanding the importance of screen savers

Methods of delivery of security awareness include the following:

- Promotional trinkets with security information such as desk calendars, mouse pads, coffee cups, note pads, etc.
- Motivational slogans such as - SECURITY is not Complete without U! These can be placed on posters or the promotional trinkets
- Login access banners
- Videos
- Weekly emails and event specific emails
- Monthly newsletters

Using a variety of methods will ensure that attention is not lost.

Periodic security training should include topics such as the following:

- Understanding applicable laws and regulations
- Understanding institution security policies and how to follow them
- Knowing how to spot employee misuse of information systems
- Understanding the process for shredding documents
- Understanding confidentiality classifications of institution data

The topics listed above are not a conclusive list and awareness programs and security training must be tailored to each institution. It may be advantageous to bring in expert help to develop an initial awareness program and to conduct periodic security awareness presentations or specific training.

In closing, this newsletter is another example of providing awareness. In the case of this newsletter our goal is to raise the reader's awareness that creating an atmosphere of security is a necessary component of

a financial institution's overall security program.

Regulators encourage the use of outside consultants to provide security testing, training, and in providing an objective view of an institution's security controls and strategies. Compushare is a professional services firm that has provided hundreds of financial institutions with that outside help. For more information on how Compushare can help you assess your risk, develop an atmosphere of security, or develop a security strategy, please contact your local Client Solutions Executive.

COMPUSHARE OFFERS A SINGLE SOURCE SOLUTION FOR:

Network Planning, Design, Configuration and Documentation

Information Security

GLBA Compliance Consulting

LAN/WAN Infrastructure Services

Network Operating System Upgrades and Conversions

Information Technology Policies and Procedures

Business Continuity

IMPORTANT COMPUSHARE NUMBERS:

So. California	(714) 427-1000
Sacramento	(916) 631-1581
San Francisco	(415) 955-0514
Las Vegas	(702) 990-3250
Houston	(713) 267-2325
Dallas	(972) 401-4150