Security Awareness Program Best Practice

Security awareness should be conducted as an on-going program to ensure that training and knowledge is not just delivered as an annual activity, rather it is used to maintain a high level of security awareness daily. This best practice is based on the work of PCI DSS council.

2.1 Assemble the Security Awareness Team

The first step in the development of a formal security awareness program is assembling a security awareness team. This team is responsible for the development, delivery, and maintenance of the security awareness program. It is recommended the team be staffed with personnel from different areas of the organization, with differing responsibilities representing a cross-section of the organization. Having a team in place will help ensure the success of the security awareness program through assignment of responsibility for the program. The size and membership of the security awareness team will depend on the specific needs of each organization and its culture.

2.2 Determine Roles for Security Awareness

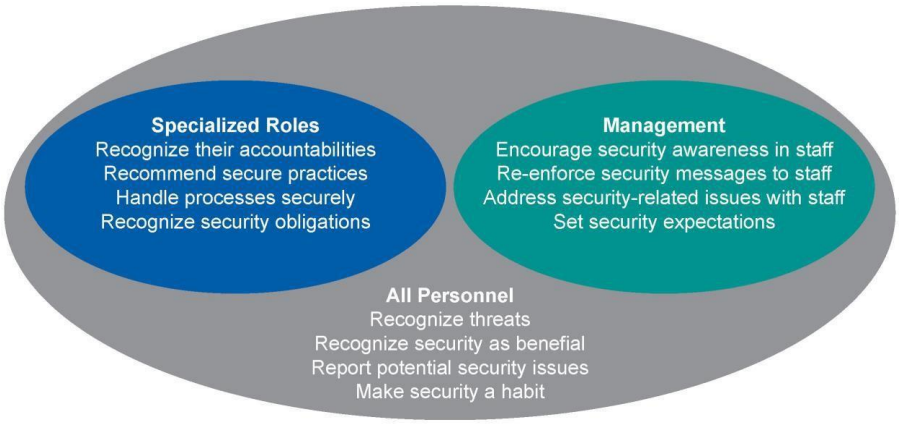
Role-based security awareness provides organizations a reference for training personnel at the appropriate levels based on their job functions. The training can be expanded upon—and subject areas combined or removed—per the levels of responsibility and roles defined in the organization. The goal is to build a reference catalogue of various types and depths of training to help organizations deliver the right training to the right people at the right time. Doing so will improve an organization's security as well as help maintain PCI DSS compliance. Whether the focus is a singular, holistic, or a tiered approach, the content can be scoped to meet an organization's requirements.

All types of roles may not apply to all organizations, and some roles may need to be divided into subsections to align with responsibilities. This can be modified according to the requirements of the organization.

2.2.1 Identify levels of responsibility

The first task when scoping a role-based security awareness program is to group individuals according to their roles (job functions) within the organization. A simplified concept of this is shown in Figure 1 on the following page.

Figure 1: Security Awareness Roles for Organizations



The diagram above identifies three types of roles, All Personnel, Specialized Roles, and Management. A solid awareness program will help All Personnel recognize threats, see security as beneficial enough to make it a habit at work and at home, and feel comfortable reporting potential security issues. This group of users should be aware of the sensitivity of data even if their day-to-day responsibilities do not involve working with sensitive data.

Additional training for those in Specialized Roles should focus on the individual's obligation to follow secure procedures for handling sensitive information and recognize the associated risks if privileged access is misused.

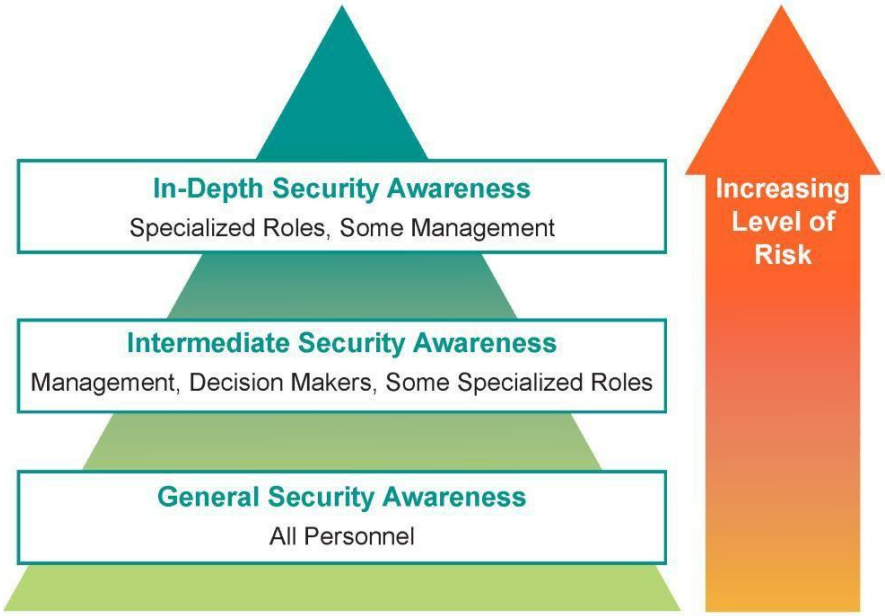
Management has additional training needs that may differ from the two previous areas. Management needs to understand the organization's security policy and security requirements enough to discuss and positively reinforce the message to staff, encourage staff awareness, and recognize and address security related issues should they occur. The security awareness level of management may also need to include an overall understanding of how the different areas fit together. Accordingly, managers of staff with privileged access should have a solid understanding of the security requirements of their staff, especially those with access to sensitive data. Management training will also help with decisions for protecting the organization's information.

2.2.2 Establish Minimum Security Awareness

Establishing a minimum awareness level for all personnel can be the base of the security awareness program. Security awareness may be delivered in many ways, including formal training, computer-based training, e-mails and circulars, memos, notices, bulletins, posters, etc. The security awareness program should be delivered in a way that fits the overall culture of the organization and has the most impact to personnel.

The following diagram depicts how the depth of awareness training should increase as the level of risk associated with different roles.

Figure 2: Depth of Security Awareness Training



2.3 Security Awareness throughout the Organization

The key to an effective security awareness program is in targeting the delivery of relevant material to the appropriate audience in a timely and efficient manner. To be effective, the communication channel should also fit the organization's culture. By disseminating security awareness training via multiple communication channels, the organization ensures that personnel are exposed to the same information multiple times in different ways. This greatly improves how people remember the information presented to them. Content may need to be adapted depending on the communication channel—for example, the content in an electronic bulletin may be different than content in an instructor-led training seminar, even though both have the same underlying message. The communication channel used should match the audience receiving the training content and the type of content, as well as the content itself.

Electronic communication methods can include e-mail notifications, eLearning, internal social media, etc. It is important to target electronic security awareness notifications to the appropriate audience to ensure the information is read and understood. It is easier for electronic notifications to go unread or ignored by busy personnel. By targeting the material and communication channel to relevant personnel, the security awareness team can improve adoption of the security awareness program.

Non-electronic notifications may include posters, internal mailers, newsletters, and instructor-led training events. In-person security awareness events that involve active participation by personnel can be extremely effective. Audience size in an instructor-led presentation is important: the larger the group, the greater risk that content may not be communicated effectively, as individuals may lose focus on the material presented if they do not feel engaged. Including activities that engage the audience, such as scenario-based activities, helps ensure the concepts are understood and remembered. For example, a structured social-engineering exercise will teach personnel quickly how to identify a social-engineering attack and react appropriately. Internal seminars, training provided during lunch breaks (commonly called "lunch-and-learns" or "brown bag"), and employee social events are also great opportunities for the security awareness team to interact with personnel and introduce security concepts. Appendix B provides a list of the common methods to communicate security awareness throughout the organization.

It is recommended that communication of security awareness be included in new-hire processes, as well as role changes for existing personnel. Security awareness training may be combined with other organizational requirements, such as confidentiality and ethics agreements. Each job position in the organization should be identified based on level of data access required. See Section 2.2, Determine Roles for Security Awareness, for more information. To ensure that the security awareness team is notified whenever a role identified as needing security awareness is filled, it is recommended this step be included in the process for all new-hire/re-classifications. Inclusion in the new-hire/re-classification process ensures the overall training goals are promoted without reliance on individual organizational units.

Management leadership and support for the security awareness program is crucial to its successful adoption by staff. Managers are encouraged to:

- Actively encourage personnel to participate and uphold the security awareness principles.
- Model the appropriate security awareness approach to reinforce the learning obtained from the program.
- Include security awareness metrics into management and staff performance reviews.