Chapter 34- IFPO - CPO Security Awareness

Purpose

Security Awareness is vital to an organization's and a security professional's progress and success. The lack of interaction between the employer and employee can lead to breeches in the overall protection of the client and resources.

Security Awareness

- The practice of security awareness operates best when a reasonable plan is put together with policies and procedures that support a comprehensive team concept.
- Managers should formulate a plan that emphasizes enlisting every employee to form partnerships with critical external partners to build a diverse team.
- This creates an environment that reduces liability risk and loss prevention by encouraging general safety practices and strategies that produce lasting results.

What is “Security Awareness”?

- “Security awareness,” is the need to focus attention on security throughout the organization and to keep security in the forefront and consciousness of every employee’s mind during the day, so the employees are making more secure decisions.
- It is letting everyone know in the organization how security impacts them and how important they are, as stakeholders and team members to the continued success of the company.
- Security awareness provides a framework of established policies and procedures that participants employ by reporting unsafe conditions, suspicious activity, and noticing general safety breaches, merely as second nature.
- Security awareness is one of the four essential components of an effective security program:
  - Physical, electronic and design security
  - Security staff
  - Security policies, procedures and protocols
  - Security education and training

What is “Security Awareness”?

- Security awareness is the first step that precedes the education and training elements of the security program.
- For business invitees, licensees and other visitors/guests, and even trespassers, the security awareness effort may be as simple as a warning sign or as complex as a signed document regarding premises security guidelines.
- Security awareness efforts interface and integrate with the entire security program of an organization to present a seamless and streamlined system to reduce or eliminate the security and crime threats faced by the organization.
- To succeed, support from the top management of the organization for security awareness is critical.
- Team members are trained and polled regularly to heighten their awareness about changing trends in practices and rapidly advancing technology.
- Along with physical awareness, security initiatives must include internal matters, like avoiding workplace violence, enhancing personal safety, and being up-to-date on the latest information technology, including safe Internet practices.

Partnerships

- To be effective, the security department should instill “security awareness” among members from all layers of the organization as well as external partners.
- Value is added to the security plan by using proven ideas from experienced external contributors.
- Employees must be encouraged to report security problems and correct safety potential issues when observed.
- Use a *double loop* communication model, which means that information should not only flow from the top of the organization down but should also flow back up to the top.
- It is in this way that outdated procedures are discovered and corrected.

Double Loop Learning

- In this theory, the organization becomes a “learning organization” by detecting and correcting errors through questioning and modification of existing norms, procedures, polices, and objectives.
- With a double loop learning security awareness communication model, a mechanism is instituted which provides feedback from employees on improving security awareness.
- By creating double loop communication, employees can then become stakeholders who have a vested interest in the success of the security awareness effort.

Techniques to Increase Security Awareness

- To greatly increase security awareness, members from all layers of the organization and external partners, should be instilled with a sense of partnership through interactive activities.
- All employees should be apprised of the organization's policies and procedures upon entering the organization.
- Organizational policies and procedures should be clear, concise, and written correctly. They should also be reviewed and updated annually, at a minimum.
- Repetition and reinforcement of the security awareness message will lead to increased involvement.
- Repetition and reinforcement can be accomplished by such methods as daily exposure using posters, weekly exposure via e-mails, and monthly or quarterly exposure through newsletters and handouts.
- Security awareness meetings should be held with all departments at least every quarter or more frequently if new issues arise or breaches occur.

Communication

- For an effective and efficient operation to exist in an organization, management should create and foster an open climate in communication.
- Utilizing only a verbal-down (management to staff) method of communication will not result in an optimal communication environment and will not furnish the breadth and depth of security awareness necessary for an organization.
- An organization requires all types of communications to be effective. These types include:
  - **Verbal-down**: Orders to perform a certain specific duty from a supervisor to a subordinate.
  - **Verbal-up**: Information from the subordinate to the supervisor on a better way to perform the duty.
  - **Written-down**: Handbooks, policy and procedure manuals, and newsletters.
  - **Written-up**: Organizational process for sending written questions, suggestions and concerns to management.

Communication

- **Written-horizontal**: Written information going from peer-to-peer. Example: The Director of Security writes to the Director of Human Resources concerning a new standard for hiring Security personnel.
- **Verbal-horizontal:** Information from meeting sessions both intradepartmental(security department only) and interdepartmental (other departments within the organization).
- A critical component of this open climate in communication is the need for action based on the information developed by these methods and strategies.
- Action by management on the information from these methods of communication will signal that the organization is listening and responding to the concerns of the staff, encouraging future communication.