Security Awareness Training

Contents

1. Introduction

Spectrum Analysis acknowledges the need for security awareness training and the importance of this area of our business. In order for Spectrum Analysis to meet standard business practices, a formal security awareness program is in place.

A robust and properly implemented security awareness program assists Spectrum Analysis with the education, monitoring, and ongoing maintenance of security awareness within the organization.

This policy focuses primarily on the following best practices:

- **Organizational Security Awareness:** A successful security awareness program within an organization may include assembling a security awareness team, role-based security awareness, metrics, appropriate training content, and communication of security awareness within the organization.

- **Security Awareness Content:** A critical aspect of training is the determination of the type of content. Determining the different roles within an organization is the first step to developing the appropriate type of content and also helps determine the information that is included in the training.

1.1. Importance of Security Awareness

One of the biggest risks to an organization's information security is often not a weakness in the technology control environment. Rather it is the action or inaction by employees and other personnel that can lead to security incidents—for example, through disclosure of information that could be used in a social engineering attack, not reporting observed unusual activity, accessing sensitive information unrelated to the user's role without following the proper procedures, and so on. It is therefore vital that organizations have a security awareness program in place to ensure employees are aware of the importance of protecting sensitive information, what they should do to handle information securely, and the risks of mishandling information. Employees' understanding of the organizational and personal consequences of mishandling sensitive information is crucial to an organization's success.

1.2. Intended Audience

The training is applicable to all staff working at Spectrum Analysis.

1.3. Terminology

Data Loss Prevention (DLP) Scanning: A process of monitoring and preventing sensitive data from leaving a company environment.

Phishing: A form of social engineering where an attempt to acquire sensitive information (for example, passwords, usernames, payment card details) from an individual through e-mail, chat, or other means. The perpetrator often pretends to be someone trustworthy or known to the individual.

Privileged Access: Users who generally have elevated rights or access above that of a general user. Typically, privileged access is given to those users who need to perform administrative-level functions or access sensitive data, which may include access to cardholder data (CHD). Privileged Access may encompass physical and/or logical access.

Social Engineering: An attack based on deceiving users or administrators at the target site—for example, a person who illegally enters computer systems by persuading an authorized person to reveal IDs, passwords, and other confidential information.

2. Best Practices in Organizational Security Awareness

Security awareness is conducted as an on-going program to maintain a high level of security awareness on a daily basis. Protecting data forms part of the organization-wide information security awareness program. Ensuring staff is aware of the importance of data security is important to the success of a security awareness program.

2.1. Security Awareness Team

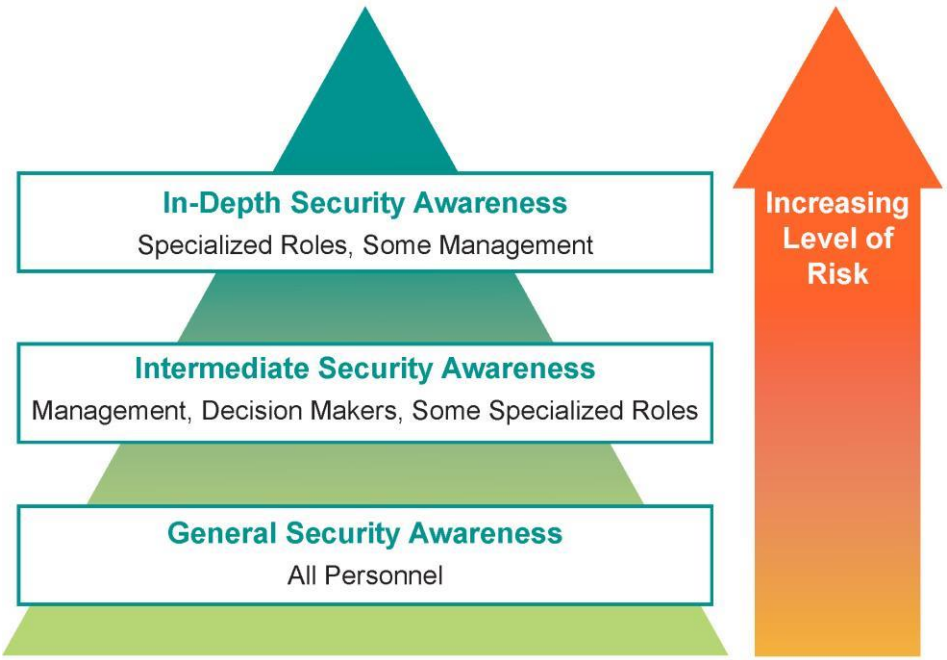
Anubhav Tewari – Chief Data Scientist

Van Pham – Senior Analyst

2.2. Minimum Security Awareness

Establishing a minimum awareness level for all personnel is the base of the security awareness program. Security awareness is delivered in many ways, including formal training, computer-based training, e-mails and circulars..

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



3. Training course agenda to be undertaken with all staff

- Organization's Security awareness policy
- Impact of unauthorized access (for example: to data, systems or facilities)
- Importance of strong passwords and password controls
- Secure e-mail practices
- Secure practices for working remotely
- Avoiding malicious software – viruses, spyware, adware, etc.
- Secure browsing practices
- Mobile device security including BYOD
- Secure use of social media
- How to report a potential security incident and who to report it to
- Protecting against social engineering attacks
    - In Person – Physical Access
    - Phone – Caller ID Spoofing
    - E-mail – Phishing, Spear Phishing – E-mail Address Spoofing
    - Instant Messaging
- Physical security
- Shoulder Surfing
- Dumpster Diving

4. Record of security training

Name	Type of security training	Completion date	Trainer