

Security Awareness Training

Implementation Guide



Overview

- Perform Assessment
- Develop Strategy
- Define Roles and Responsibilities
- Determine Frequency
- Create Content
- Deliver Training
- Measure Effectiveness

Perform Assessment

- Determine if any security awareness components exist within the organization
 - May be piece of another training program
 - May be able to leverage existing pieces
- Determine if awareness program infrastructure exists
 - Are there other awareness programs
 - The programs may serve as a template

Develop Strategy

- Base awareness strategy on organization's goals and objectives
- Be sure to note that it is not just an IT issue
- Review existing policies
 - Add cyber security to existing policies
 - Create policies if none exist
- Create awareness program learning objectives

Define Roles and Responsibilities

- Information Owners
 - Those who have been given the responsibility of determining
 - the value of data
 - Who is allowed to access the information
- System Users
 - All users including contractors and vendors
- System Administrators
 - Those who maintain the integrity and privacy of the information
 - Those who grant actual access

Determine Frequency

- New hire training
 - Upon hire
- Management Level
- All Users
 - annually
- Contractors
 - Prior to working on system
 - Annual refresh
- Refresh when an event occurs

Create Content

- Start with Policies
 - Create policy awareness
- Focus awareness on any incidents or events that occur
- Include appropriate reporting of events and incidents
- Create award program for recognition of good security practices

Deliver Training

- Log Banners
- Media, CD hard copy
- Audio
- Note pads
- Awareness Posters
- Mouse pads

Measure Effectiveness

- Annually
- Use metrics such as
 - Total number of employees who attended training
 - Percentage of employees who attended training