

2. Information Security Awareness Program

2.1 Prerequisite Knowledge

Participants in this course should have a basic knowledge of information security principles. There are no other prerequisites.

2.2 Course Objectives

You will learn:

- Information Security Awareness concepts and terminology
- How to plan and organize an Information Security Awareness program in your organization
- How to focus and tailor your program to your organization's specific needs
- Identify best practices for developing, implementing and maintaining your awareness program
- Develop metrics to measure the effectiveness of your awareness program

2.3 Course Description

This course addresses one of the most important and often ignored aspects of information security. Participants will learn the importance of developing an information security awareness program in their organizations and how to go about developing and implementing one. Participants will walk through the steps of identifying areas inside their organizations that require an awareness program. Participants will learn how to develop an information security awareness program according to their organization's needs and capabilities. Participants will understand the various methods of communicating the security awareness message to every part of the organization.

2.4 Course organization

The course consists of four modules of four hours each that are taught over a two day period.

2.5 Course Topics

1. Considerations Before Developing the Information Security Awareness Program
 - 1.1. Know your environment and corporate culture
 - 1.2. Getting buy-in, who holds the power and who will be your allies
 - 1.3. What department communicates with the employees and how will you use this infrastructure to your benefit
 - 1.4. Where are the information security weaknesses in your organization
 - 1.5. Communicating your message to your organization
 - 1.6. The document review (Policies, Procedures, Standards, Guidelines)
2. Implementing the Information Security Awareness Program
 - 2.1. Distribute documentation
 - 2.2. Standards and procedures should be available electronically

- 2.3. Provide a shortened version of these documents with more detail provided via hyperlink or drill down.
- 2.4. Leverage any existing newsletters or electronic bulletins for your ISAP
- 2.5. Communicating your message
- 2.6. Use posters and trinkets
- 2.7. Banner advertisements
- 2.8. Companies in the business of helping you get the message out
3. What to put into your presentation
 - 3.1. Basics of what should go in the ISAP presentation
 - 3.2. Presentation examples
4. Additional Considerations
 - 4.1. What departments do you need on your side
 - 4.2. Other sources of information
5. ISAP Evaluation
 - 5.1. Develop metrics to evaluate your program and make changes when needed
 - 5.2. When you are successful let everyone know
 - 5.3. Develop a quiz that employees must pass annually – update it each year
 - 5.4. Have employees renew their security agreements every 2 years
 - 5.5. Create a Virus Response Team that can respond to virus outbreaks and answer employee questions
6. Human Firewall Project
 - 6.1. What is the Human Firewall Project? (www.humanfirewall.com) Goals
 - 6.2. The Blueprint:
 - 6.3. Get Management Buy-in
 - 6.4. Assign and Clarify Roles and Responsibilities
 - 6.5. Create an Action Plan with a Budget
 - 6.6. Develop or Update Security Policies
 - 6.7. Develop an Information Security Awareness Program
 - 6.8. Measure your Progress
 - 6.9. Adapt and Improve your Awareness Program based on Feedback
 - 6.10. Develop an Incident Response Team and Plan
 - 6.11. Assign a manager and include needed expertise on the team.
7. The Top Ten Most Common Mistakes
8. Summary and Conclusions