



Information Security Awareness Program Proposal

Michael E. Whitman, Ph.D.



Purpose

The purpose of information security awareness is improving coherence of the need to protect information and system resources, and defining the user's role in the process.

Making computer system users aware of their security responsibilities and disseminating correct practices can help user's change past behaviors.



Benefits

There are two overriding benefits of awareness, namely:

- (1) improving employee compliance and
- (2) increasing the ability to hold employees accountable for their actions.

One principal purpose of information security awareness is to reduce errors and omissions.

However, it can also reduce fraud and unauthorized activity by increasing employees' knowledge of accountability and the penalties associated with such actions.



Accountability

Both the *dissemination* and the *enforcement* of policy are critical issues that are strengthened through awareness programs.

Employees cannot be expected to follow policies and procedures of which they are unaware.



Awareness

Awareness stimulates and motivates those being trained to care about security and to remind them of important security practices.

Explaining what happens to an organization, its mission, customers, and employees if security fails motivates people to take security seriously.



Awareness

Awareness can take on different forms for particular audiences.

Awareness is used to reinforce the fact that security supports the mission of the organization by protecting valuable resources.

Awareness is also used to remind people of basic security practices, such as logging off a computer system or locking doors.



Comparative Framework

Comparative Framework

	AWARENESS	TRAINING	EDUCATION
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Objective:	Recognition	Skill	Understanding
Teaching Method:	<u>Media</u> - Videos - Newsletters - Posters, etc.	<u>Practical Instruction</u> - Lecture - Case study workshop - Hands-on practice	<u>Theoretical Instruction</u> - Discussion Seminar - Background reading
Test Measure:	True/False Multiple Choice (identify learning)	Problem Solving (apply learning)	Essay (interpret learning)
Impact Timeframe:	Short-term	Intermediate	Long-term

Figure 13.1 compares some of the differences in awareness, training, and education.



Awareness

- ◆ Effective security awareness programs need to be designed with the recognition that people tend to practice a *tuning out* process (also known as *acclimation*).
- ◆ For this reason, awareness techniques should be creative and frequently changed.



Program Implementation

Step 1: Identify Program Scope, Goals, and Objectives.

Step 2: Identify Training Staff.

Step 3: Identify Target Audiences.

Step 4: Motivate Management and Employees.

Step 5: Administer the Program.

Step 6: Maintain the Program.

Step 7: Evaluate the Program.



Step 1: Identify Program Scope, Goals, and Objectives.

Scope:

- Faculty, Staff and Students in offices, labs and public access ports.

Goals:

- Increase the general level of security awareness.
- Reduce the incidences of computer fraud, waste and abuse.
- Create a more security savvy member of the organization's computing community.



Step 1: Identify Program Scope, Goals, and Objectives.

Objectives:

- Design a detailed security awareness implementation plan.
- Create interesting security awareness materials using internal resources whenever possible.
- Provide variety and creativity in the program.
- Have program in place and functional within 6 months of approval.



Step 2: Identify Training Staff.

Primary administrator responsible for program is the Chief Information Security Officer.

Assistance will be provided by key security faculty, University outreach training professionals, and select system administrators.

Some assistance will be available on a temporary basis from students in Information Security coursework.



Step 3: Identify Target Audiences.

There are three target audiences:

- Students
- Staff
- Faculty

Within these three audiences there are two general categories of users:

- Managerial users – those responsible for managing technology and users of technology.
- End users – those using technology.



Step 4: Motivate Management and Employees.

This will be accomplished through a series of short presentations on the importance of security and the security awareness program.



Step 5: Administer the Program.

- ◆ The program will consist of three main efforts:
 - Security awareness presentations.
 - Security awareness columns in campus newsletters and other dedicated publications.
 - Security awareness materials:
 - Posters
 - Videos
 - CD-ROMs
 - Promotional Materials



Program Theme

Be SAFE



Think before you Click!

Security Awareness For Everyone





Security Awareness Program

- ◆ Step 6: Maintain the Program.

Maintenance will be provided through a joint effort between the CISO, faculty, and selected Information Security students.

- ◆ Step 7: Evaluate the Program.

Evaluation of the program will be conducted on a semi-annual basis by the CISO.



Costs

How to Spend a Dollar on Security recommends that out of every security dollar you spend:

- 15 cents: Policy
- 40 cents: Awareness**
- 10 cents: Risk Assessment
- 20 cents: Technology
- 15 cents: Process

We feel it can be done for much less, for an estimated annual budget of approx \$5,000.

Many materials (posters, newsletters etc.) will be contributed by security personnel and students.

by Patrick McBride (ComputerWorld November 9, 2000)