



How to Win Management Support for Awareness



Thomas R. Peltier
How to Win Management Support for Awareness
27 April 2008



Abstract

- Here is the trick: learn first about management's needs, then take best advantage. Talk policy, "compliance" and risk reduction" rather than training and awareness."
- Learn how to tie awareness initiatives to key business needs, using seven case studies that will illustrate varied goals and approaches. Leave with strategies for interacting more effectively and confidently with management.



Thomas R. Peltier
How to Win Management Support for Awareness
27 April 2008





Introduction

- Development of security policies, standards, procedures and guidelines are only the beginning of an effective information security program.



Thomas R. Peltier
How to Win Management Support for Awareness
27 April 2008



Frequently Asked Questions

- What is asset classification?
 - Asset classification is the process of assigning value to data in order to organize it according to its sensitivity to loss or disclosure.



Thomas R. Peltier
How to Win Management Support for Awareness
27 April 2008





Frequently Asked Questions

- What the reasons to classify data?
 - Information is an asset and the property of the organization.
 - Because resources are limited, it is important to prioritize the areas that need protection.
 - Not all information is of equal value.
 - Establish accepted levels of behaviors when handling certain types of information.
 - Assist employees with protecting data.



Thomas R. Peltier
How to Win Management Support for Awareness
27 April 2008



Frequently Asked Questions

- What common classifications?
 - **Sensitive:** Limited in use for a selected group or process.
 - **Restricted:** Information that is related to departmental business operations, but not available for public consumption.
 - **Public:** Information that requires no special protection or rules for use .



Thomas R. Peltier
How to Win Management Support for Awareness
27 April 2008



Frequently Asked Questions

- Who “owns” the data?
 - The act of quantifying the importance of data is a BUSINESS responsibility.
 - All portions of information created by users need to be defined as to the level of importance to the organization.
 - Managers should work with users to understand the mission-critical aspects of their information and processes.

Frequently Asked Questions

- What are employee responsibilities?
 - **Owners:** responsible for judging the value of the information resource and assigning the proper classification level.
 - **Custodians:** administering access requests to information authorized by the owner.
 - **User:** use the information for the purpose intended (follow the rules).

Frequently Asked Questions

- What is the classification process?
 - Define the “Owners”, “Custodians” and “Users” of the data.
 - Create data classification policy including access levels.
 - Catalogue data based on rules of use and ownership.
 - Record data owners, custodians and users.
 - Audit data classification scheme for compliance.

Introduction

- A strong security architecture will be rendered less effective if there is not a process in place to make certain that the employees are aware of their rights and responsibilities.
- All too often, security professionals implement the “perfect” security program, and then forget to include the personnel into the formula.



Introduction

- In order to be as successful as possible, the information security professional must find a way to sell this product to the customers.
- A effective security awareness program could be the most cost effective actions management can take to protect its critical information assets.

Key Goals

- For security professionals there are three key elements for any security program: *integrity, confidentiality and availability.*
- Management is concerned that information reflects the real world and that they can have confidence in the information available to them so that they can make informed business decisions.
- One of the goals of an effective security program is to ensure that the organization's information and its information processing resources are properly protected.



Key Goals

- The goal of confidentiality extends beyond just keeping the bad guys out, it also ensures that those with a business need have access to the resources they need to get their job done.
- Confidentiality ensures that controls and reporting mechanisms are in place to detect problems or possible intrusions with speed and accuracy.



Thomas R. Peltier
How to Win Management Support for Awareness
27 April 2008



Key Goals

- An effective information security program must review the business objectives and/or the mission of the organization and ensure that these goals are met.
- Meeting the business objectives of the organization and understanding the customers' needs are what the goal of a security program is all about.
- An awareness program will reinforce these goals and will make the information security program more acceptable to the employee base.



Thomas R. Peltier
How to Win Management Support for Awareness
27 April 2008



Key Goals

- As important as the written word is in defining the goals and objectives of the program and the organization, the true fact is that most employees will not have the time and/or desire to read these important documents.



Key Goals

- 5 Key Elements
 - An awareness program to ensure that the message is identified as important will get to all of those that need it.
 - Identify individual (s) responsible for the implementation of the security program.

Key Goals

- 5 Key Elements
 - The ability to classify information assets according to their relative value to the organization is the third key element in an information security program.
 - Implementation of the basic security concepts of separation of duties and rotation of assignments.

Key Goals

- Most Important
- Active management support



Presentation Keys

- While every organization has its own style and method for training, it might help to review some important issues when creating an awareness program.
- One very important item to keep in mind is that the topic of information security is very broad.

Presentation Keys

- Do not get overwhelmed with the prospect of providing information on every facet of information security in one meeting.
- The old adage of “How do you eat a elephant? One bite at a time” must be remembered.





Presentation Keys

- Prioritize your message to the employees.
- Start small and build on the program.
- Remember you are going to have many opportunities to present your messages.
- Identify where to begin, present the message, reinforce the message and then build to the next objective.



Thomas R. Peltier
How to Win Management Support for Awareness
27 April 2008



Presentation Keys

- Keep the training sessions as brief as possible.
- It is normally recommended to keep these session to no more than 50 minutes.
 - There are a number of reasons for under an hour; biology (you can only hold coffee for so long), attention spans and productive work needs.
- Start with an attention grabbing piece and then follow up with additional information.



Thomas R. Peltier
How to Win Management Support for Awareness
27 April 2008



Presentation Keys

- Tailor the presentations to the vocabulary and skill set of the audience.
- Know who you are talking to and provide them with information they can understand.
- This will not be a formal doctoral presentation.

Presentation Keys

- The awareness session must take into account the audience and the culture of the organization.
 - Understand the needs, knowledge and jobs of the attendees.
- Stress the positive and business side of security, protecting the assets of the organization.
- Provide the audience with a reminder (booklet, brochure or trinket) of the objectives of the program

Presentation Keys

- Start with an introduction of the topic of what information security is about and how it will impact their business units and departments.
- Follow with a video that will reinforce the message and present the audience with an external expert supporting the corporate message.

Presentation Keys

- Discuss any methods that will be employed to monitor compliance to the program and provide them with the rationale for the compliance checking.
- Provide them with a time for questions and ensure that every question either gets an answer or is recorded and the answer will be provided as soon as possible.
- Finally, give them some item that will reinforce the message.

Examples

- The basics
 - Each implemented a classification policy
 - Each identified at least three audiences
 - Senior management
 - Owners
 - User community

Company 1

- Multi-national pharmaceutical corporation
 - Created policy
 - Conducted facilitated session
 - Used results to train employee base





Company 2

- Multi-national manufacturing corporation
 - Implemented policies and practices
 - Conducted focus sessions to verify practices
 - Created awareness sessions – trained the trainers
 - Followed up with Internal Control Review Questionnaire



Thomas R. Peltier
How to Win Management Support for Awareness
27 April 2008



Company 3

- Insurance Company
 - Facilitated session to create policy
 - Facilitated session to verify policy
 - Sent overview e-mail to all employees
 - Conducted classification sessions with business unit groups
 - Identified owner
 - Information record and description
 - Retention period
 - Classification



Thomas R. Peltier
How to Win Management Support for Awareness
27 April 2008



Company 4



- Utility Company
 - Implemented policy
 - Established Business Unit Information Security Coordinators
 - Trained coordinators
 - Implemented information security awareness module for new employee orientation
 - Compliance check through quarterly coordinator's meetings

Company 5

- Multi-National Petroleum Corporation
 - Implemented policy
 - Sent overview e-mail to all employees
 - Conducted classification sessions with business unit groups
 - Identified owner
 - Information record and description
 - Retention period
 - Classification



Company 6



- Bank
 - Implemented policy
 - Sent overview e-mail to all employees
 - Conducted classification sessions with business unit groups
 - Identified owner
 - Information record name and description
 - Classification
 - Annual follow-up session

Company 7



- Multi-Media Corporation
 - Assessed policy
 - Edited policy
 - Conducted facilitated session to verify edits
 - Prepared roll-out outline
 - Identified follow-up process

Summary

- Information security is more than just policies, standards, procedures and guidelines.
- It is more than audit comments and requirements.
- It is a cultural change for most employees.
- Before any employee can be required to be compliant with a security program, they first must become aware of the program.
- Awareness is an ongoing program that employees must have contact with on at least an annual basis.

Summary

- Information security awareness does not require huge cash outlays.
- It does require time and proper project management.
- Keep the message in front of the employees.
- Use different methods and means.
- Bring in outside speakers whenever possible and use videos to your best advantage.

CSISX
SECURITYEXCHANGE

Comments?



Questions?

Critiques!

Thomas R. Peltier
How to Win Management Support for Awareness
27 April 2008

CSI
COMPUTER
SECURITY
INSTITUTE

CSISX
SECURITYEXCHANGE

How to Win Management Support for Awareness

Peltier
Associates

Thomas R. Peltier
How to Win Management Support for Awareness
27 April 2008

CSI
COMPUTER
SECURITY
INSTITUTE