FISSEA News & Views

January 2006

Letter from the Chair

Dear FISSEA,

I will open by wishing each of you a Happy New Year. 2005 was a year to remember and we hope that 2006 will be better. What with severe hurricanes, earthquakes, war, Tsunamis, and other difficulties, the negatives seem to take priority over positives. Thankfully, 2006 is starting out right as our NIST Executive Assistant, Peggy Himes is enjoying the role of first-time Grandmother and our News&Views Editor, Nan Poulios, is also preparing to become a first-time Granny. Guess this goes to show the power of the press and value of publications such as this in conveying all kinds of information. Can you see the segue?

We do want to thank Nan for helping out in the Editor's chair. Articles, when received, are almost in final stage but need the careful eye on shpelling and grammour as well as validation of facts in order to produce a quality product. It is our sincere hope that you find News&Views worth reading. And we know that you budding authors have lots of insights to offer our membership, so please send submissions to Nan. Our next issue will come out shortly before the annual conference, so get them in soon.

If you haven't yet signed up for FISSEA's 19th Annual Conference, please do so. Conference directors Curt Carver and Will Suchen have a grand slate of presenters to satisfy your intellectual and practitioner sides. By now, you may have seen one of the outstanding on-line conference ads posted by MaryAnn Strawn and have hopefully shared the info with others who would benefit. This year's conference brochure, under the watchful eye of Patrice Boulanger, is quite appealing. Oh, and Gretchen Morris has extended the due date until the 24th of February so you still have time to submit trinkets, posters, and websites to our competition.

Regarding websites, we are going to be updating our's, with the aid of Patrick O'Reilly. If you have suggestions for improvements, please send them to Patrick, Peggy, and/or me. Technologically, we also thank Mark Wilson for his moderation of discussion threads on our FISSEA list-serve. Questions asked and subjects which have been discussed are often thought provoking. FISSEA thanks Joan Hash and NIST management for her support and for permitting the participation on the part of Peggy, Mark, Patrice, and Patrick. It is also worthy of note that Mark was the Master of Ceremonies for an 800-16 working session, hosted by the FORUM of Computer Security Program Managers. If you did not attend, your insights are still being sought. Please send recommended additions and changes to Mark and/or myself. All submissions will be considered in the ongoing plan to update this landmark document.

Looking back on this past year, I can honestly say that our hard working 2005-6 Exec Board has met the test. First timers K Rudolph, Susan Hansche, and Jim Litchko are learning the ropes from Jeffrey Seeman, Tom Foss, and our most excellent Assistant Board Chair, Barbara Cuffie. These competent, well meaning, volunteers give of themselves to attend meetings and plan such activities as our free workshops and annual conference. So, the organization is in capable hands. Hands which I hope you will get to shake during our 2006 Conference.

In closing, let me state that we are always looking for a few good folks to help carry the load. If you are so inclined and willing to do so, please submit your name for the Exec Board election.

Looking forward to seeing you on 20 and 21MAR2006,
Louis

Request for Comments

By Louis Numkin

Yesterday, I was fortunate enough to attend and participate in the first Special Workshop on Proposed Changes to NIST SP800-16 "IT Security Training Requirements: A Role- and Performance-Based Model." NIST's Mark Wilson with assistance from Tanya Brewer made an excellent presentation on the background, FISMA and OPM requirements, NIST Learning Continuum Model, and related issues. From comments which I have received, their leadership was very well appreciated.

You may recall that I posted a request for suggested changes to all members of the FISSEA list some time back. Replies were shared with NIST and Joan Hash has thanked FISSEA for the input.

In light of yesterday's discussions, permit me to again pose the following question to our FISSEA membership:
“Have you any comments, and/or suggestions, regarding the organization and content of SP800-16? “

"Now is the time..." to submit your thoughts on how the pending revised guidance could be made more understandable, usable, and worthwhile to practitioners. It is up to each of us to express ourselves so as to help NIST create a meaningful and functionally sound document.

Please take the time to send me any words for SP800-16, so they may be considered as direction and/or for inclusion. Whether you have already spoken to people about them or even if you sent them to us before, please respond to this request.

Subject Matter Experts Needed: CompTIA Security+ Exam Workshop

By Carol Balkcom

CompTIA periodically holds workshops to do routine exam maintenance on its certifications. Volunteer subject matter experts, who are not trainers, are needed for these workshops. For CompTIA's Security+ exam, a 4-day workshop is being held outside Chicago on January 23rd, and a second, 3-day workshop on February 21st. We are looking for a few additional *security* subject matter experts for one or both of these workshops in order to hold them as scheduled.

These are the requirements:

- Must be Security+ certified;
- Must have a minimum of 3 years work experience in security;
- Must not be a trainer/teacher of security;
- Must be able to handle your own transportation and accommodations to/in Chicago during the workshop.

Familiarity with the domains and objectives (which will not change) of the Security+ exam are also required. A modest honorarium and most meals are provided. More information and application are provided below. If you qualify and are interested, please contact us right away, and thank you--

http://enews.comptia.org/certification/SecuritySME.htm

FISSEA Conference "Training for a Cyber-Secure Future"

By Peggy Himes

The annual conference is approaching. Program Co-Chairs, Curt Carver and Will Suchan are assembling a two-day agenda to rival other much more expensive conferences. We would like your assistance in advertising, please go to the FISSEA website, http://csrc.nist.gov/fissea, download the flyer and distribute it in your office. Board member, K Rudolph did a spectacular job in creating the flyer. Electronic registration is currently available, go to https://rproxy.nist.gov/CRS. A vendor exhibition will return on March 20th, please contact Liz Hood at the Federal Business Council, liz@fbcinc.com, 1-800-878-2940 x227. The preliminary agenda will be posted soon.

FISSEA Conference "Training for a Cyber-Secure Future"
March 20-21, 2006
Bethesda North Marriott Hotel & Conference Center, Maryland
Registration fee $340
Electronic registration https://rproxy.nist.gov/CRS

FISSEA Poster, Website, and Trinket Contest submissions are due by February 4, 2006 and may be sent to fissea-contest@nist.gov. Board member, Gretchen Ann Morris is coordinating this contest. Nominations for the FISSEA Educator of the Year Award are due by February 3, 2006, please send nominations to peggy.himes@nist.gov. Detailed information on how to enter the contests and to view past winners are available on the FISSEA website. The conference brochure will be snail-mailed in January.

This message is coming to you through a one-time alias and not through the FISSEA list-serve. You will not be able to respond to this message. Should you want to contact FISSEA, please send a message to fisseamembership@nist.gov. You may contact individual board members through their email addresses listed on the website. The FISSEA Board Chair may be contacted at louis.numkin@irs.gov. Of course, if you are on the listserve you can continue to communicate with all registered members; complete details are on the website.

We hope many of you will take the opportunity to register for the conference early and will download the flyer and share it with your colleagues.

Prizes Needed for 2006 FISSEA Conference

By Jim Litchko

In 2006, the FISSEA Conference will be held in Rockville, Maryland, on March 20-21. A key to having a successful conference is the new knowledge and friends that you leave with and the special gifts and prizes that contributes to the conference experience. This also provides companies and organizations an opportunity to be recognized for contributing items and services in support of the conference. In the past, contributions have included:

- Conference Support Items (need 150)
  - Notebooks
  - Security reference materials - books, roadmaps, CDs, etc.

- Prizes - To be raffled off during the conference
  - Computer security posters
  - Books
  - Registrations to training courses
  - Speaker presentations for security events
  - Study guides for CISSP exams
  - Subscriptions
  - Products - firewalls, security tools, authentication tokens, ipods, laptops, etc.
  - Memberships
  - Certification Test Fees

If your organization is interested in contributing items like the above, please contact Jim Litchko at 301-661-3984 or jim@litchko.com soon.

Your support will be greatly appreciated.

Security Poster, Trinket & Website Contest

By Gretchen Ann Morris

Showcase the items you use to help keep your users aware via the security themes or messages presented in each poster, trinket or website submitted.

We will spotlight the winners with the FISSEA community! Below are the rules for the contest:

Rules and Guidelines

This contest includes Awareness, Training and Education posters, trinkets (pens, sewing kits, stress relief items, t-shirts, etc.) and websites. Each category of the competition will be judged separately. A winner will be selected from each category and awarded a certificate at the annual FISSEA conference.

1. RULES

a. Only one item in each category may be submitted (1 poster, 1 website, and/or 1 trinket). However, an individual or organization may enter in all three categories.

b. The entries must be submitted by a FISSEA member prior to the deadline of February 4, 2006.

c. Entries must have a security education theme and be part of the organization's current security awareness program. All entries must be original and wholly unclassified.

d. A Contest Entry Form must accompany all entries and is available on the FISSEA website http://csrc.nist.gov/fissea. Each submission automatically agrees to allow FISSEA to publish, however, only the winning entries will be published on the FISSEA web page.

e. PowerPoint will be used to prepare each entry. One slide will be designated the Entry Form for the category followed by the entry for that category. All slides should be e-mailed to: fissea-contest@nist.gov.

f. Any item not adhering to the rules and entry guidelines will be ineligible. The decision of the contest supervisor is final.

2. GUIDELINES

a. A committee of at least three FISSEA members will judge the contest. The judges will evaluate each category (poster, website and/or trinket) on the basis of originality, security message, and graphic concept.

b. The winners in each category will be announced at the FISSEA Conference. A certificate will be awarded to each winner with a congratulatory letter signed by the FISSEA Executive Board Chairperson.

The Human Side of Section 508

By Trevor J Osgood and Russ Mumford

Introduction

We all need to be cognizant of our responsibilities to make our web sites and software accessible to all users. We've all heard of Section 508 and a lot of us are probably scared of it. It's impossible to read or interpret not only for the layperson but also for the majority of decision makers. In this series of 4 articles, we'll put a human face on Section 508 and return the dialogue to good, old-fashioned common sense. Section 508 isn't a construction manual; it's a set of abstract standards with some (obsolete) examples. By the time we're done, you'll know the basic terminology, the concepts they represent and you'll be a more informed decision maker.

A Brief Perspective on Website Accessibility.

Let's look at this from a historical perspective. Initially, web designers tended to be young, bright-eyed go-getters. Lacking many precedents for the new medium of the Internet, they designed web sites that looked good to them. The result was frequently something that was "intuitive" for a 20-something who spends all his spare time playing video games. For many of "the rest of us", understanding and using these web sites presented a challenge. It also quickly became apparent that they were impossible for a great many persons with common disabilities.

The Downfall of Inaccessible Web Sites And Software.

This is a lamentable condition. Being able to interact with the world and to obtain basic services online should be a high priority. We can deliver many services more economically and immediately online which are less costly for the public to obtain and can be delivered to remote areas 24x7x365. And when we talk about economy, we're talking about public citizens, not just institutional budgets.

We can all see what a great thing wheelchair access to our public buildings is for the wheelchair-bound. Now imagine the time and expense saved for that person if they can obtain the same services and never have to leave the house.

How Many People Are Affected With Disabilities?

These examples can be misleading. Most of the disabilities we encounter that make it difficult to use the web aren't as extreme as immobility. A lot of them are age-related issues that most of us will face in our lifetimes. It's commonly held that 20% of the population is affected with a disability of some sort. The figure remains relatively static from year to year. In itself, this represents a large portion of our population. If we look at percentages of disabled persons in various age groups, we get a better idea of how many persons in our specific audience are affected with disabilities.

Age Group	Percent with Disability
All Ages	19.7%
Under 15 years	7.8%
15 to 24 years	10.7%
25 to 44 years	13.4%
45 to 54 years	22.6%
55 to 64 years	35.7%
65 years and over	54.5%

U.S. Census Bureau: Americans with Disabilities
http://www.census.gov/hhes/www/disable/sipp/disab97/ds97t1.html

Clearly, if we're communicating to groups of adults, we can estimate that between 1/4 and 1/2 of our audience is challenged by inaccessible websites. Alas, the older we get, the more difficulties we may have.

The Range Of Disabilities Affecting Web and Software Users.

Despite the broad range of disabilities affecting website accessibility, we can categorize them into four basic groups: Cognitive/behavioral, Visual, Mobility and Auditory.

- Cognitive/behavioral disability includes extreme disability such as autism, but also more common disabilities such as dyslexia, a language-based learning disability (about 15-20% of us have them) or Attention Deficit Disorder (4-6% of population) http://www.interdys.org/servlet/compose?section_id=5&page_id=95 - How%20common%20are%20language-based%20le http://www.add.org/articles/factsheet.html.

I also have to note, with some chagrin that about 60% of our population reads at a 6th-grade-or-below comprehension level. Clearly, part of accessibility involves neither speaking nor writing over people's heads. http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=1999470

- Visual disabilities include folks who require glasses, color-blind (a surprising 6% of the population), partially blind persons, or blind people. http://www.stlukeseye.com/Conditions/ColorBlindness.asp
- Mobility challenges can include partial to full paralysis, fine-motor coordination challenges and disease-related challenges such as the palsy that accompanies Parkinson's disease.
- Auditory dysfunction such as deafness or common age-related hearing loss can affect the online experience particularly with multimedia presentations.

What We've Learned.

Fortunately, we've made great progress in developing web technologies that are accessible to persons with these broad spectra of disabilities. What we've learned has also allowed us to create standardized approaches to information presentation so that's it's easier for the rest of us to work with and understand. These technologies are lighter-weight than previous web development techniques, so they offer greater accessibility to persons with slow, dial-up Internet connections, a key accessibility metric. The new approach is called Standards-Based Web Development but the principles exactly parallel any software development project.

And Some Good News.

Not only is the information we see and interact with on the web evolving, the browsers that most of us use to access it are getting better and we as Internet users are getting better at using them. What this means to you is that a good deal of what is written in Section 508 is obsolete, has been shown to be "a bad idea" or simply doesn't present itself as a problem all that often these days.

For the length of this series on Section 508, Greenidea, Inc. and dataSpheric will be moderating an online discussion where we hope to answer some of your more specific questions. Please drop by ask your questions and add your viewpoint. The address for the forum is: http://www.dataSpheric.com/services/508/forum/

Trevor J Osgood, trevor@dataSpheric.com
Russ Mumford, Mumford@greenidea.com

Implementing an Information Security Awareness Program

By Tom Peltier

(Reprinted from Journal Information Systems Security, Volume 14, Number 2).

Overview

An effective information security program cannot be implemented without implementing employee awareness and training program to address policy, procedures and tools. Learning consists of three key elements:

- Awareness – which is used to stimulate, motivate and remind the audience what is expected of them.
- Training – is the process that teaches a skill or the use of a required tool.
- Education – specialized, in-depth schooling required to support the tools or as a career development process.

The article addresses the elements that make up a successful information security awareness program. We will address the role organization personnel play in the information security program and how to use this information to your benefit. We will discuss how to establish awareness program scope; how to segment the audience; and how to ensure content is effective in getting the message to the user community.

Introduction

Development of information security policies, standards, procedures and guidelines is only the beginning of an effective information security program. A strong security architecture will be rendered less effective if there is not a process in place to make certain that the employees are made aware of their rights and responsibilities with regard to organization information assets.

All too often security professionals implement the "perfect" security program, and then are surprised that it fails because they forgot to sell their product to their constituents. In order to be successful, the information security professional must find a way to sell this product to the customers.

For years I have heard information security professionals discuss their jobs in terms of overhead, as if this is some evil thing. Nearly every employee within an enterprise is overhead. Even the CEO, CFO, CTO and CIO are all overhead. However, they have learned what we need to learn, and that is that we all add value to the bottom line of the enterprise. Our task, just like the big "C"s is to ensure that the business objectives or mission of the enterprise is met. What the information security professional has failed to do is to sell the services of information security.

We must examine our services such as risk analysis, policies, procedures, standards, vulnerability assessments and business continuity planning and determine how each of these services supports the business objectives. Before you can be effective, you will need to take stock of the services your team offers and prepare your own unique sales pitch for management.

Key Elements of a Security Program

The information security triad of *confidentiality, integrity and availability* drive the security program. Management, however, is concerned that information reflects the real status of the organization and that they can have confidence in the information available to them can be used to make informed business decisions. An effective information security program endeavors to ensure that the organization's information and its processing resources are available when authorized users need them.

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 perform their job. Confidentiality ensures that controls and reporting mechanisms are in place to detect problems or possible intrusions with speed and accuracy.

An effective security program must take into account the business objectives and/or mission of the organization and ensure that these goals are met as safely and securely as possible. Understanding the customer's needs must be the first step in establishing an effective information security program. The awareness program must reinforce these objectives and will make the program more acceptable to the employee base.

As important as a set of written policies, standards and procedures are in defining the architecture of the security program and the infrastructure that supports it, the true fact of the matter is that most employees will not have the time and/or desire to read these documents. The objective of the awareness program is to take the message to the people.

The information security program has five key elements that must be presented to the audience. These include:

- A process to take the message to the user community to reinforce the concept that information security is an important part of the business process;
- Identification of the individuals that are responsible for the implementation of the security program;
- The ability to determine the sensitivity of information and the criticality of applications, systems and business processes;
- The business reasons why basic security concepts such as separation of duties, need-to-know and least privilege must be implemented; and

- That senior management supports the goals and objectives of the information security program.

Believe in What <u>You</u> are Doing

Before you can begin to put together a program to sell information security to your fellow employees, you must first sell the product to you. Many information security professionals hear either directly or indirectly that the role they are performing is overhead and that it inhibits the other employees from meeting their assigned objectives. The part about overhead is true, but so are the vast majority of employees. The "C" level employees (CEO, CFO, CTO, CISO, etc.) are all overhead. However, they have a charter that establishes their legitimacy and describes how they support the business objectives or mission of the organization.

You will need to have a charter published, but more importantly you will have to persuade yourself that what you do adds value to the organization. When ever I am teaching a class on information security issues I always give the attendees a homework problem. The exercise is to come up with four things that you, as a security professional, do to help your enterprise meet its business objectives or mission. These four items should be expressed in non-security, non-technical, non-audit terms. Use the language of the business unit managers to express your four value-added statements.

When creating your value added statements, do not state that you "add users to the system using ACF2". Instead, sell your services by stating that you ensure that authorized users are given access to information resources in a timely and efficient manner. Tell your audience what it is that you do that enables them to do their job.

Just as you have to prepare to sell your job and its duties to management and fellow employees, so must you be prepared to sell the services that you provide. Again these services must be presented to the user community in the language they understand. *Security requirements* or *audit requirements* are not part of the business process and they do not exist. There are only business objectives or mission requirements. So when we present our services, we must use the terms that management uses.

> *Risk Analysis* – Risk analysis is a technique used to identify and assess factors that may jeopardize the success of a project or achieving a goal. This process is also known as project impact analysis. This process will include a cost-benefit analysis and typically incorporates the features and benefits of the asset or process under review.
>
> *Risk Assessment* - Organizations use risk assessment to determine what threats exist to a specific asset and the associated risk level of that threat. The threat prioritization (establishing the risk level) provides the organization with the information needed to prioritize where to implement appropriate controls measures, safeguards or counter measures to lower the risk to an acceptable level.

Policies – Management establishes its goals and objectives for protecting the assets of the enterprise by implementing policies. Policies are used to introduce the concepts of what is expected of all employees when using enterprise assets and what non-compliance can lead to. The message of the policies are also included in the contract language so that third parties are aware of their responsibilities.

With policies implemented along with an awareness program, the enterprise than can seek relief in the courts, if necessary, to protect their assets. Policies establish the behavior expected of all personnel granted access to that asset.

Procedures – These are probably the easiest security measure to explain return on investment. Procedures are the step by step process used to complete a task. They provide users with the information needed to complete a task and ensures to management that the tasks are being completed in a uniform and approved manner. Procedures improve efficiencies in employee work-flow and assist in the prevention of misuse and fraud.

Standards – Remember Y2K, that historical event that caused many of us a lot of extra work? It was lack of standards or the ignoring of standards that made management spend so much money to retrofit the fixes. Standards are a way of ensuring that programs and systems will work together and that when there is a need to do error searching, the people looking through old code will be better able to understand what is out there.

By establishing standards the enterprise limits rouge applications, systems, platforms, hardware or software. There is less time spent in supporting non-standard activities or products. When a new application or system is moved into production, the existing systems and applications will not have to make modifications to handle non-standard information or data. Standards are a cost savings process that support the efficient running of the enterprise.

Business Continuity Planning – Since the events of September 11, 2001, most organizations have seen the need to implement an enterprise-wide continuity plan. Management has always been charged with a fiduciary responsibility to protect the assets of the enterprise. BCP is a process that allows management to show that they have exercised due diligence with respect to the information processing resources and assets. By having a plan and testing the plan, the enterprise is showing to employees, stakeholders and interested third parties that the continued operation of the enterprise has been addressed and is taken seriously.

While these are only examples of how to sell your information security services, they do provide you with the idea of how this can and should be done. To be successful, the information security professional must step into the role or the businessperson. Security is a portion of the entire business process and must use the words and objectives of the business units to be successful. Our goal is not just to have security endure, but we want it to prevail. To do this we must become an active voice in the business or mission of our organizations.

Program Goals

Employees want to know what is expected of them and who to turn to for assistance. The ongoing information security awareness program will provide those answers to the user community. The employees need to understand the security program is the supported, approved and directed by senior management.

Another key goal of an awareness program is to ensure that all personnel get the message. The process should begin with new employee orientation and continue through the final exit interview. In between there should be at least annual mandatory refresher classes and sessions.

Contract personnel need to be made aware of the information security program goals and objectives, but be caution when considering whether or not to include third parties in regular employee training and awareness sessions. Normally, your organization would want the contract house to conduct the awareness training for their personnel. At least, hold separate awareness sessions for contract personnel. Be sure to work with the Purchasing and Legal departments to ensure that the language of the contracts specifies adherence to the security program.

All too often the programs fail because there is little or no follow up. There is usually the “Big splash” kickoff and then not much else. Over the years management and employees have been trained how to respond to the big event and that is to do nothing.

In the 1970’s management and employees were introduced to a concept termed “Quality of Work Life (QWL)”. This bold new concept was to address how employees felt about the job, their bosses and fellow employees. Management would then take steps to improve the work atmosphere. In the 1980’s we were introduced to “Total Quality Management (TQM)” where we discovered that employees were our most important asset and that they needed to be empowered. In the 1990’s we were trained in the “Learning Organization” and were introduced to the concept of the “Ladder of inference”. What management and employees learned from these concepts was that the best way to deal with any new program is to wait. Expend the least amount of energy as possible and there is a good chance that it will go away or die due to inaction.

The employees know that inaction or indifference is the best tool to use when confronted with a new initiative. To be successful it will be necessary to map out a strategy to keep the message in front of the user community on a regular basis. When mapping out your program, you might want to consider incorporating special dates into the calendar of events. For an information security program consider doing something on the following dates:

- May 10 – International Emergency Response Day

- September 8 – Computer Virus Awareness Day
- November 30 – International Computer Security Day

However, keeping the message in front of the user community is not enough. The message must make the issues of information security come alive and become important to all who see the message. This can be accomplished in part by finding ways to tie the message in with the goals and objectives of each department. Every department has different needs and objectives. The message you bring must address those needs.

Find ways to make the message important to the employees. When discussing controls, identify how they help protect the employee. For example: When requiring employees to wear identification badges, many security programs tell employees that this requirement has been implemented to meet security objectives. What employees should be told is that the badges ensure that only authorized persons have access to the work place. The goal of this security measure is to protect the employee in the work place by ensuring that only authorized personnel have access. When presenting controls present the message to the employees in a manner that shows them the benefit.

Finally, the security program is meant to reduce losses associated with the intentional or accidental disclosure, modification, or destruction of information or the denial of services from the systems or applications. This can be accomplished by raising the consciousness of the user community of the ways to protect information and the processing resources. By ensuring that these goals are met, the organization will be able to improve employee efficiency and productivity.

Segmenting the Audience

To be successful, the awareness program should take into account the needs and current levels of training and understanding of the employees and audience. Typically there are five key ways to establish an effective segmentation of the user audience:

- Current level of computer usage;
- What the audience really wants to learn;
- How receptive the audience is to the security program;
- How to gain acceptance; and
- Who might be a possible ally.

Current Level of Computer Usage

To assess the current level of sophistication in computer usage, it will be necessary to ask questions of the audience. While sophisticated workstations may be found in employees work areas, their understanding of what these devices cab do may be very limited. Ask questions as to what the tasks area and how the tools available are used to support these tasks. It may come as a surprise to find out that the newest and most powerful system on the floor is being used as a glorified 3270 terminal.

Be an effective listener. Listen to what the users are saying and scale the awareness sessions to meet their needs. In the awareness field, one size or presentation does not fit all.

What Does the Audience Really Want to Learn?

One way to get the audience open to listen to the security message is to provide them with awareness training on topics that are in the news. My team and I would watch for news shows such at “Dateline” or “48 Hours” or the evening news to run a segment on some current issue. We would purchase a copy of that segment and make it available to the departments for their staff meetings. We did this initially with phone card theft and cell phone cloning. While these issues were not actually part of the information security program, we were able to tie a brief information security message into the presentation.

In today’s environment the concern over identity theft is a perfect lead into the issues surrounding information security. So take the time to find out what the concerns are of the user community and tap into those needs to present your message.

Determine How Receptive the Audience Is

Identify the level of receptiveness to the security program. Find out what elements are being accepted and which ones are meeting resistance. Examine the areas of non-compliance and try and find ways to either alter the requirement or find a better way to present its objectives. Do not change fundamental information security precepts just to gain unanimous acceptance, this is an unattainable goal. Make the program meet the greater good of the organization and then attack the pockets of resistance to lessen the impact.

One method of determining levels of receptiveness is to conduct a “walkabout”. A walkabout is conducted after normal working hours and looks for certain key indicators:

- Offices locked;
- Desks and cabinets locked;
- Workstations secured;
- Information secured; and
- Recording media (diskettes, tapes, CDs, USB drives, etc.) secured.

Seek Out Ways to Gain Acceptance

Work with the supervisors and managers to understand what their organization’s needs are and how the program can help them. Remember, it is their program. It will be necessary for you to learn to speak their language and understand their specific needs. No single awareness program will work for every single business unit or department. You must be willing to make alterations to the program and show a willingness to accept suggestions.

The best way to gain acceptance is to ensure that the employees and managers are partners in the security process. Never submit a new control or policy to management without sitting down with them individually to discuss and review the change. By knowing what each department or business unit does, you will be able to present the change to the manager and discuss how it will help them meet the goals and objectives.

It will also be important to know the peak activity periods of the various departments and what the manager's chief concerns are with regard to meeting objectives. When meeting with the managers, be sure to listen to their concerns and be prepared to ask for their suggestions on how to improve the program. When I was starting out in the security business, I ran into managers that had "an issue" that they wanted resolved. When I came back with the resolution, I often found that they had "another issue". After working this process a couple of iterations, I found that the best way to prevent "additional issues" was to be prepared for the "issues" list. I would answer item number one and, if presented, item two. If the manager went to a third item, I would ask if there were any additional "issues". This would allow me to get all of the items out and then move forward.

Possible Allies

Find out which managers support the objectives of the security program and those that have the respect of their peers. Look beyond the physical security and audit departments. Seek out the business managers that have a vested interest in seeing the program succeed. Use their support to springboard the program to acceptance.

When discussing the security program, avoid referring to it as "my program". Senior management has identified the need for a security program and has tapped you as their messenger and catalyst to move the program forward. So when presenting the program to user groups, employees and managers, refer to the program as "their program" or as "our program". Make them feel that they are the key stakeholders in this process.

In a presentation used to introduce the security program to the organization, it may be beneficial to have the CEO or President introduce the subject through a video and saying something like the following:

> "Just as steps have been taking to ensure the safety of the employees in the workplace, the organization is now asking that the employees work with us to protect our second most important asset – information. If the organization fails to protect its information from unauthorized access, modification, disclosure and/or destruction, then the organization faces the prospect of loss of customer

> confidence, competitive advantage and possibly jobs. All employees must accept the need and responsibility to protect our intellectual property and processing resources."

Involve the user community and accept their comments when ever possible. Make the information security program their program. Use what they identify as important as a key to the awareness program. By having the users involved, then the program truly becomes theirs and they will be more willing to accept and internalize the process.

Program Development

As we discussed above, the awareness presentation will vary based on the needs of the audience. Not everyone needs the same degree or type of information do their jobs. An awareness program that distinguishes between groups of people and presents only information that is relevant to that particular audience will have the best results.

The job category is one way to segment the awareness audience and will provide the presenter with guidelines as to type and duration of presentation. A standard presentation should typically last no longer than forty-five minutes and should consist of a combination of live discussion and video tape or movie information. This form and length of presentation is fine for employees and line supervision.

Business unit managers have two or more departments or groups reporting top them and have less time. Schedule an individual twenty minute meeting with these managers and have two or three pages of materials to use to support your discussion. Stress the objectives of the program and how the program can be used by the business unit to meet its objectives.

Senior management (including officers and directors) will have about fifteen minutes available for the presentation. Have a one page summary for them and discuss how the program supports them in their fiduciary duty and how it helps them meet their due diligence obligation.

Contractors and other third parties will need their own awareness sessions and they typically following the format of employees and line supervision presentations. When ever possible, segregate third parties form the awareness training of regular, full-time employees. This will help to ensure that the message for third parties is consistent and that there is no confusion as to their job status.

Once the audience has been segmented, it will be necessary to establish the roles that the users will be expected to assume. These roles may include managers acting as the information owner. Service providers (either internal or external) acting as custodians of the intellectual property and general users.

For any message that is to be delivered, be sure to employ the *KISS* (Keep It Simple, Sweetie) practice. You will have other opportunities to present material to the user community. Don't try and present all the information security goals and objectives in one session. Remember you have only about thirty minutes of attendee attention.

Inform the audience but try and stay away commandments or directives. Discuss the goals and objectives using real world scenarios. Use antidotes to reinforce the concept that problems can happen here and that they do. A good story will be remembered long after the session is over. Quoting policies, procedures, standards and/or guidelines will turn off the audience quickly. Policies and procedures are boring; if employees want more information, give them a reference card to help them find the resource.

Try to avoid telling employees that something is being implemented to "be in compliance with audit requirements". This is at best a cop-out and fails to explain in business terms why something is needed. The awareness session presents management's beliefs and objectives for the use and protection of the organization's information resources.

Methods to Convey the Message

How do people learn and where do people obtain their information? If you can answer these questions then you awareness program will have a better chance for success. Depending on what needs to be accomplished in the learning process, the manner in which the message is to be conveyed may be different. If we were implementing a training program we would be able to select from three basic methods of training:

- Buy a book and read about the subject;
- Watch a video on the subject; or
- Ask someone to demonstrate the process

For most employees the last method is preferred for training. Most people like the hands-on approach and want to have someone there to answer questions.

With an awareness program the process is a little different. In awareness we want to raise consciousness about an issue. Awareness is to stimulate and motivate the audience about an issue or objective. It will be necessary to tap into the method most used by our audience to receive information. According to the *USA Today*, over 90% of the people obtain their news and information from television and/or radio. To make an awareness program work it will be necessary to use this delivery model.

Knowing how people learn will help us in implementing an effective security awareness program. Neural-linguistic programming is study of how people learn. This process has identified three basic ways in which people learn. These are:

- Auditory – these people have to hear something in order to grasp it.
- Mechanical – this learning-type must write down the element to be learned. Those taking notes during meetings are typically mechanical learners.

- Visual – this type of learner, of which 90% of our audience is, need to see a picture or diagram to understand what is being discussed. People that learn via this method normally have white boards in their office and use it often.

Because so many of our employees use the television as their primary source for gathering information, it is important to use videos and other visual stimuli to reinforce the message. Visual models can include posters, pictures and videos. The use of videos serves several purposes.

With the advent of the news magazine format so popular in television today, our employees have become conditioned to accept the information presented as factual. This allows us to use the media to present them with the messages we consider important. Because the audience accepts material presented in this format, the use of videos allows use to bring in an “informed” outsider to present the message. Many times our message fails because the audience knows the messenger. Being a fellow worker, our creditability may be questioned. A video provides an “expert” on the subject.

There are a number of organizations that offer computer and information security videos. As we discussed above, consider having a senior executive videotape a message that can be run at the beginning of the awareness session. However, be very careful when considering developing your own twenty minute security video. Costs for creating a quality in-house video of twenty minutes can exceed $100,000.

An effective awareness program will also take advantage of brochures, newsletters, or booklets. In all cases the effectiveness of the medium will depend on how well it is created and how succinct the message is. One major problem with newsletters is finding enough material to complete the pages each time you want to go to press. One way to present a quality newsletter is to look for vendors that provide such services. Typically, the vendor supplies the textual material for the newsletter and the company can put its logo and masthead on the newsletter with space for a small column of specific information.

Many organizations are de-centralizing the information security responsibility and requiring each business unit to establish an information security coordinator. One of the tasks of this individual is to present the awareness sessions to their specific organization. An effective method of getting a consistent message out using this format is to “train the trainers”.

The security awareness presentation is typically created by the central information security group and then regional training sessions are held to present the message and tools to the unit coordinators. During this half-day session, the key concepts are reinforced and the coordinators work with the security team to customize the session for their needs. This method helps ensure that the message presented meets the overall need of the organization and that the business unit feels that the message is directed toward their requirements.

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. When creating your awareness program, remember that the topic of information security is very broad. Try not to get overwhelmed with the prospect of providing information on every facet of the information security program in one meeting. The old adage of “How do you eat an elephant? One bite at a time” must be adhered to.

Prioritize the message to the user community. This will require that there be a risk assessment performed on the information security infrastructure that will provide the organization with a prioritized list security issues. Select the most pressing issue from this list or a topic that the Information Security Steering Committee has identified as vital.

The information security awareness program is an continuous process and you will have many opportunities to present the security messages. Identify where to begin, present the message, reinforce the message and then build to the next objective. Keep the awareness sessions as brief as possible. It is normally recommended to keep the sessions to no more than fifty minutes. There are a number of reasons for under an hour, biology (you can only hold coffee for so long), attention spans and productivity issues.

Start your session with an attention grabbing piece such as the chief executive’s video message or even an ice-breaker “personality test”. One that I use is quite simple one to start some sessions:

<table>
<tr><th colspan="3">Personality Test</th></tr>
<tr><td colspan="3">Using word association techniques, write down the first response that comes into you head when you hear each of the following words:</td></tr>
<tr><td><b><i>Term</i></b></td><td></td><td><b><i>Meaning</i></b></td></tr>
<tr><td><i>Dog</i></td><td></td><td>How you view your own personality</td></tr>
<tr><td><i>Cat</i></td><td></td><td>How you view your partner’s personality</td></tr>
<tr><td><i>Rat</i></td><td></td><td>How you view your boss’ personality</td></tr>
<tr><td><i>Ocean</i></td><td></td><td>How you view your own life</td></tr>
<tr><td><i>Coffee</i></td><td></td><td>How you view your <b>LOVE</b> life</td></tr>
</table>

Tailor the presentation to the vocabulary and skill set of the audience. Know who you are talking to and provide them with information they can use and understand. This is not to have the appearance of a doctorial dissertation.

The awareness session must take into account the audience and the culture of the organization. Understand their needs, knowledge and what the jobs of the attendees are. Knowing what the attendees do for a living will assist the presenter in striking a relationship with them.

Stress the positive and business side of security. Just as we discussed in selling security, you will have to sell them the concept that security is good for them. I often use the following analogy when discussing this issue. At the end of World War II, some GI's found that people living in areas of Europe lived for years beyond what Americans did. One of the factors in this long life was their eating of yogurt. So these GI's decided to introduce yogurt to the American culture. One major problem, plain yogurt has a nasty taste. To be successful, the GI's had to find a way to make it palatable to the American taste. So they added fruit to the bottom of the cup and Americans could then stir up their good-tasting yogurt.

Information security is plain yogurt. To most of our employees it leaves a bad taste in their mouth. You are going to have to find a way to make the message palatable to the user community. This is done by understanding their needs and adjusting the message to meet their issues. Reinforce the message by providing booklets, brochures or trinkets with the message or slogan.

Presentation Format

While every presentation will be different, the following format is provided as a starting point for you to use to develop you awareness presentation.

Introduction

Start with an introduction of the topic and how the security program will support them in the completion of their tasks and jobs. This is where the senior management video would also be presented.

Message

Follow the introduction with the message. Typically this would either be a live presentation (see Effective Communication Tips) or the information security video.

Compliance Issues

Discuss any methods that will be employed to monitor compliance to the security objectives and provide the audience with the rationale for such compliance checking.

Questions and Answers

Provide the audience with about ten minutes for questions and answers. Ensure that every question is recorded and the answer is provided during the session (which is best) or where the answer will be posted. Use the Q & A from one session as input or background for your newsletter follow up.

Reinforce

Give then some item that will reinforce the message to them when they are back in their work areas.

Effective communication

An effective information security program will depend on how well the message is communicated to the audience. While many of us are confident in the importance of the message we will be presenting, often times the message is missed because of other factors. To be as effective as possible, it might be helpful to identify potential barriers to effective communication.

- **Image** - Dress as the audience is dressed, only a little better. While many organizations have converted to the business casual dress, when you are presenting, it is important to exhibit the proper respect and professionalism to your audience. I once worked for a company that was headquartered in the Pacific northwest. I had just finished 22 years with a global manufacturer located in the mid-west and they had just begun business casual. I was shocked at the attire of my fellow employees. I believe it is know as "grunge-rock chic". When we went to do work at the client site, I required the sales person to inform us as to how the clients dressed. I had to make sure we abandoned our avant-garde look and became more traditional. I went to a meeting one time and did not recognize my own employee, he "cleaned up real nice".
- **Prepare** - Nothing will turn an audience off quicker than a presenter that stumbles around for materials and/or looses his or her place. Make certain that all audio visual is working properly (get there early and test everything).
- **Present** - Do not read your presentation. Use bullet points or brief phrases to speak from. With any luck your audience will know how to read. Avoid reading verbatim the presentation slides. Speak to the audience as if you are having a conversation with them.

- **Jargon** - As information security professionals, we speak a very strange language. Many of us have also come from the Information Systems environment and this will compound the problem. I strongly recommend that you practice the presentation in front of a select focus group.
- **Audience** - Know your audience and speak to them in terms they will understand. Each and every department has its own language. Do your homework and learn what terms are important to them and use them correctly in your presentation.
- **TLAs** - A TLA is a Three Letter Acronym (TLA) for three letter acronyms. The next time you attend a meeting, keep a running score of the TLAs and FLAs (four letter acronyms) that a bandied about. Say what you mean and keep the TLAs to a minimum and define them before using them
- **Idioms** - Be careful with language. Our organizations have many different ethnic groups and slang terms may be misunderstood or even offensive. Be mindful of those in your audience and select your terms wisely.
- **Priorities** - As security professionals, we feel that security is the organization’s most important objective. However, Purchasing, Accounting, Payroll, Human Resources, etc. have other priorities.
- **Schedule** - Just as every department has a unique language and priorities, they also have deadlines. Schedule your presentations around their busy periods. Try to become part of a regular staff meeting if possible.
- **Time** - Keep the awareness sessions brief and businesslike. At Gettysburg, Edward Everett was the featured speaker and spoke for nearly two hours. President Lincoln spoke second and in less than five minutes and the world remembers his Gettysburg Address. Remember it is quality not quantity that will make a successful presentation.

Information security is an important part of doing business today. The message of employee responsibilities must be presented to them on a regular basis. To have a chance for success, a good presenter will be clear, concise, and brief. Know your audience and play to their needs and concerns. By doing your homework, the audience will be more open to receive the message. If they accept the message as being meaningful, then the objectives of information security will become incorporated into the business process.

When to do Awareness

Any awareness session must be scheduled around the work patterns of the audience. Take into account busy periods of the various departments and make certain that the sessions do not impact these peak periods.

The best times for scheduling awareness sessions is in the morning on a Tuesday, Wednesday or Thursday of a regular work week. First thing Monday morning will impact those getting back and starting the week’s work. Having a session on Friday afternoon will not be as productive as you would like. The bodies may be in the room, but the minds and souls have already departed. This time frame will result in the onset of the “stunned owl” syndrome. This is a process where the words no longer go in one ear and out the other. At this point the words hit the audience in the forehead and fall to the floor.

The physiological clock of humans is at its lowest productivity level right after lunch. If you turn out the lights to show a movie, make sure to turn up the volume so it can be heard over the snoring. Try to avoid the after lunch time period.

Also, schedule sessions during off shift hours. Second and third shift employees should have the opportunity to receive the message during work hours just like those on day shift.   I once did a presentation to the third shift employees after their regular shift. I was assured by their management that an hour of overtime was all they needed to stay awake. Well, one young lady dozed off as soon as the lights went out and she did not wake up until I went over to tell her everyone had gone home.

Presentation Styles

As we discussed briefly before, each group of employees require a different time frame and approach to security awareness presentations. We will review the requirements here.

Senior Management

While most other sessions will last no more than fifty minutes, senior management has less time for even issues as important as information security. Prepare a special brief, concise presentation and have available in-depth supporting documentation.

Unlike typically presentations, senior management does not want a video and personality test. They may not even want presentation slides. They generally prefer that the presenter sit with them for a few minutes and discuss the issues and how the security program will support their objectives.

Quickly explain the purpose of the program, identify any problem areas and what solutions you propose. Suggest to them an action plan. Do not go to them with a problem for which you have no solution. Do not ask them to choose a solution from several you present because they might do just that and it might not be what is needed. You are the expert here and they are expecting you to come to them with your informed opinion on how the organization should move forward.

They are expecting a sound, rational approach to information security. They will be interested in the overall cost of implementing the program and how this program bench-marks against others in the same industry or business.

Managers

These individuals are focused on getting their job done. They will not be interested in anything that appears to slow down their already tight schedule. To win them over, it will be necessary to demonstrate how the new controls will improve performance processes. As has been stressed throughout this article, the goal of security is to assist management in meeting business objectives or the overall mission.

Stress how the new processes will give the employees the tools they need (such as access to information and systems) in a timely and efficient manner. Show them the problem resolution process and who to call if there are any problems with implementation of the new process.

Line Supervisors and Employees

The employees are going to be skeptical. As we have discussed above, they have been through so many company initiatives that they have been trained to wait and hope the process will pass over. The compliance checking concept will assist in getting the message to them that information security is here to stay.

Identify what is expected of them and how it will assist them in gaining access to the information and other resources they need to complete their assigned tasks. Point out that by protecting access to information, they can have a reasonable level of assurance (remember to avoid using absolutes) that their information assets will be protected from unauthorized access, modification, disclosure or destruction.

The Message

The message to be presented will be based on whether your organization has an effective information security program in place and how active it is. For those organizations just activating the program, it will be necessary to convince management and employees of its importance. For organizations with an existing out-dated program, the key will be convincing management that there is a need for change.

The employees need to know that information is an important enterprise asset and is the property of the organization. All employees have a responsibility to ensure that this asset, like all other company assets, is properly protected and is used to support management-approved activities. The awareness program will allow employees to be made aware of the possible threats and what they can do to combat them.

The scope of the program must be made clear to the audience. Is the program limited to only computer-held data or does the program reach to all information, where ever it is found and how ever it is generated? The awareness process must ensure that employees know the total scope program. It must enlist their support in protecting this vital asset because the mission and business of the enterprise depends on it.

Summary

Information security is more than just policies, procedures, standards and guidelines. It is more than just responses to audit comments or industry requirements. It is a business process that requires a cultural change for most employees.

Before anyone can be required to be compliant with a security measure, they must first be made aware of the need and the process. This is an ongoing process that begins during new employee orientation and continues through the post employment exit interview.   It must be conducted at least on an annual basis and include regular reminders.

Information security awareness does not require huge budgets. It does require some time and proper project management. The message must be kept in front of the user community and different vehicles of delivery should be used. Use your contacts in the industry to bring in speakers to support your program and use videos whenever possible.

Before you can sell you security program to any of the employees, you must sell it to yourself. The awareness program must be the voice of reason and logic. Start small and expand. By the time the employees realize there is a security program, it will already be part of the culture.

TRAINIA:

13-14 MAR 2006: The Institute for Applied Network Security is holding a Forum at the Sheraton Tysons Corner, in Vienna, VA. Please contact Tom Lix, VP of Marketing, for more info by dialing (617)399-8100, or point your browser at www.ianetsec.com Should you speak with them, please let them know you saw this in the FISSEA News&Views newsletter.

20-21 MAR 2006: FISSEA Annual Conference "Training for a Cyber-Secure Future", Bethesda North Marriott Hotel and Conference Center, 5701 Marinelli Road, North Bethesda, MD 20852. http://csrc.nist.gov/fissea/ . Electronic registration: https://rproxy.nist.gov/CRS Conference benefits: dual tracks of high quality relevant presentations; discover new ways to improve your IT security program; gain awareness & training ideas and resources; obtain practical solutions to training problems; great networking opportunities; and a tremendous bargain for a first-class learning experience. Further questions, contact peggy.himes@nist.gov.