Strengthen Security
with an
Effective Security Awareness Program

Tom Olzak
April 2006

You've developed a world class security program. Your technology-based defenses are cutting edge. Your security team is well trained and ready to handle anything that comes its way. So you're done, right? Not quite. One of the most important pieces of an effective information asset defense is missing – employee awareness.

In this paper, I define security awareness, list the objectives of an effective awareness program, and I step through a process to build, implement, and manage on-going support of the program.

What is Security Awareness?

Awareness programs shouldn't be confused with training. Training deals with developing specific skill sets. The objective of awareness programs is to focus the attention of employees on maintaining the confidentiality, integrity, and availability of information assets. It allows them to recognize IT security concerns and respond appropriately (Wilson and Hash, 2003).

Why is Security Awareness Important to Your Business?

A security team alone can't provide the kind of overall enterprise awareness necessary to fend off the wide variety of incidents an organization might face. That kind of awareness requires the active participation of every employee in the company. Further, incidents caused by employee mistakes result in far more damage to businesses every year than external attacks. Obtaining the support and participation of an organization's employees requires an active awareness program; one that's supported by all layers of management. "Your employees are the stewards of your critical data and information assets…" (Taylor, 2004). Make sure they're up to the challenge.

A fully aware workforce is able to prevent many incidents. Unpreventable incidents are identified faster, resulting in less business impact.

Awareness Program Objectives

The key objective in any security program is the modification of employee behavior. You can't make people actively work to secure the information for which their responsible unless they want to. So you need to help them understand why it's important to them and the company. Some of the topics you should consider to meet this objective include the following:

1. What is information security?

2. What is the company's security strategy?
3. What are the company's security policies and how do they translate to practical, day-to-day activities?
4. What are our processes?
5. What regulations (local, state, and Federal) apply to business operations?
6. How does security impact the employees' day-to-day activities?
7. How would a major security incident affect the health of the business?

Another important objective of awareness training is employee understanding that management, at all layers, fully supports the company's security program. Without strong evidence of management support, your security effort is weakened and attention to information provided during awareness classes is less than enthusiastically received.

Creating an Awareness Program

According to Mark Wilson and Joan Hash at NIST, there are four steps to reaching a working awareness program: design the program, develop or purchase awareness materials, implement the program, and post-implementation activities (2003).

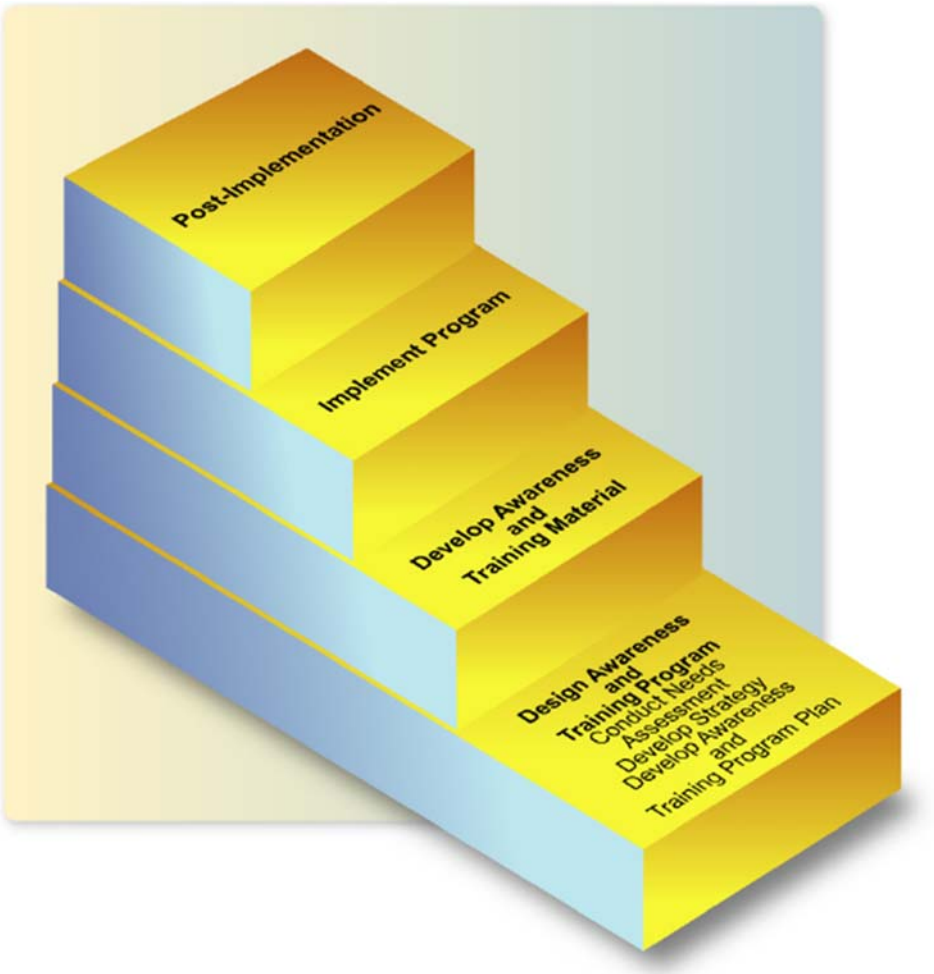

Figure 1: Steps in the Creation of a Security Awareness Program
(Wilson and Hash, 2003)

Design the program
The first step in design is determining how to structure the program. The design process begins with a needs assessment. Figure 2 depicts various inputs to the assessment.

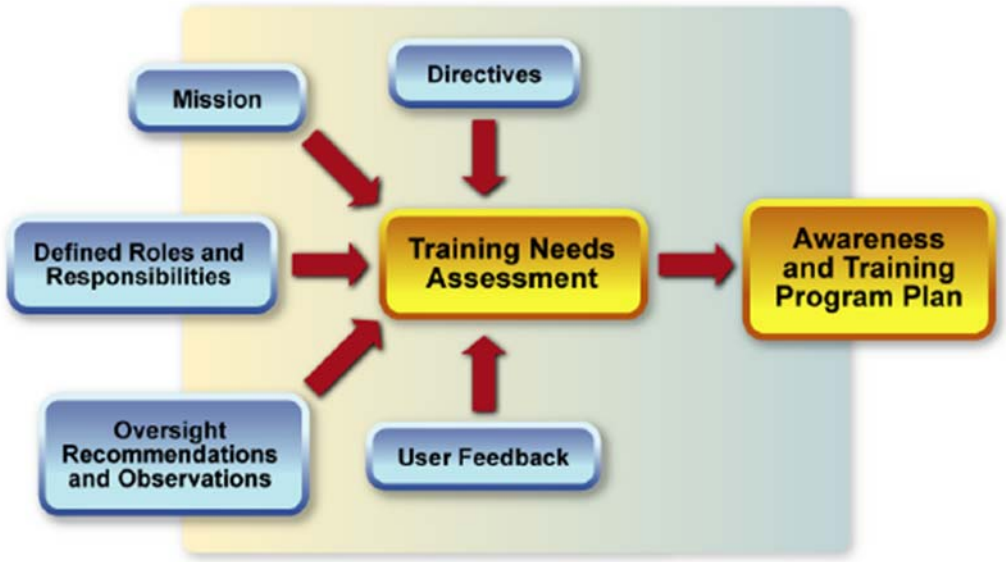

Figure 2: Inputs to Needs Assessment Process
(Wilson and Hash, 2003)

The inputs in the graphic show categories from which inputs should be solicited. Drilling down into each category, use the following guidelines to obtain the level of detail required to document and prioritize the proposed awareness topics:

Recent Incidents – The assessment of recent security incidents (within the last one to two years) provides insight into weaknesses in employee knowledge of processes or security principles in general.

Regulatory Issues – The awareness program is a good tool for supplementing your training efforts for regulations like HIPAA and SOX.

Employee Concerns – Many employees are already aware of security fundamentals. They can be a good source of information about day-to-day problems related to information asset assurance.

Management Concerns – Management's perspective is usually more operational or strategic. More emphasis is placed on investor, vendor, customer, and employee welfare overall. Management input helps to complete the picture that illustrates internal concerns about security.

Customer Concerns – With today's rising rate of identity theft, there is a growing concern among consumers about how companies protect their

information. Addressing customer concerns isn't just good business; it's the right thing to do.

Investor Concerns -- The level of investor confidence in your organization's ability to protect sensitive information (intellectual property, financial information, etc.) is directly related to your level of working capital. Be sure to see your company's level of protection from the investors' perspective.

Define training goals

Taking the results of the needs assessment, define the goals of the program. What concerns are you trying to address? Are you including overall policy, process, standards, and guidelines discussions in your sessions? How many sessions are required to cover meet your goals?

Identify target audiences

Next, identify your target audiences. Typically, awareness presentations should be delivered to three distinct groups within your organization: all employees, management, and information technology employees. The information provided varies across the three groups.

Presentations to all employees include the definition of security, how it impacts their day-to-day-activities, and some level of discussion about processes that support the security program. Make employees aware of policies and where to find them. This target audience includes *all* employees, including management and information technology personnel.

The awareness message presented to management should focus on policies and how the enforcement of them leads to overall business goals and objectives. Managers in both non-technical and technical areas should attend these sessions.

Finally, information technology professionals require awareness tools that introduce and explain standards, guidelines, and baselines. Describe how existing and future systems must be designed to assure confidentiality, integrity, and availability of data.

Frequency of delivery

Keeping security in the forefront of everything users do each day is a continuous task. Holding one-time sessions and then assuming your work is done is a dangerous approach. Over time, the impact awareness sessions have on employee behavior lessens. Repetition is the key to security awareness.

The types of awareness materials you select and the culture of your organization play a significant role in how often you bring your employees back into the classroom. For example, the use of posters, table tents in the cafeteria, or weekly awareness email or voice mail messages might result in classroom sessions once a year.

Management support
As with all security initiatives, your awareness program will never meet its goals without strong management support. Funding, employee attendance at awareness sessions, and employee perception of the importance of security all depend on support at all layers of management.

Develop or buy awareness materials
The first challenge in acquiring awareness materials is determining the behavior you're trying to reinforce. Align behavior modification objectives with the overall goals of your program.

Next, ensure your materials are easy to use, scalable to large audiences, and provide a way to track who is using them. For example, posters are a good tool, but you can't measure who—if anyone—is reading them. On the other hand, an intranet application that includes quizzes and a participant tracking database meets all three criteria. Not every awareness tool has to meet all three. A good mix of materials is usually effective and easily fits within your security budget.

In-house development
There are many security awareness materials you can easily develop in-house, including:

- Posters
- Table tents
- Email
- Intranet postings

If you have difficulty coming up with topics to support your program goals, page 24 in NIST SP 800-50 lists some suggestions. There are also many web sites that provide organizations with awareness program information. A good example is AttackPrevention.com (http://www.attackprevention.com/Security_Management/Awareness_Program).

Buy
Developing applications or classroom delivery material is often beyond the capabilities of in-house staff. In such cases, it makes more sense to look for training partners. The following is a list of companies providing a variety of products, services, and free information targeting security awareness.

Easyi (http://www.easyi.com/enus/is/solutions.asp)

Security Awareness Inc (http://www.securityawareness.com/)

Erudio Security, LLC (http://www.erudiosecurity.com)

Implement the program
Once the program is complete, it's time to roll it out. The first step in roll-out is to communicate. Let the employees know what to expect. Inform them of the importance of security awareness both to the company and to each of them personally. In other words, wrap some context around the message.

Although you might have strong management support for the *concept* of security awareness, make sure all levels of management are enrolled in the actual delivery method. Few problems can kill a large information delivery effort like the loss of management support during roll-out.

Post Implementation
After initial message delivery, it's important to measure the effectiveness of your approach. Follow the following steps to gather feedback and strengthen the message:

Monitor for compliance – Assuring compliance is the role of both audit teams and the IS Security organization. Keep metrics to determine if awareness related causes of audit deficiencies and security incidents are declining.

Obtain feedback from stakeholders – Using the same sources listed in the needs assessment section of this paper, solicit feedback about the perceived success of the program. Figure 3 shows various methods you can use.

Figure 3: Feedback Solicitation Methods
(Wilson and Hash, 2003)

Adjust the program to address weaknesses – Based on the feedback, make adjustments to your program materials and delivery methods. Since awareness

training is an on-going process, the results from monitoring and stakeholder feedback should incrementally improve over time.

Conclusion

Securing your infrastructure and applications isn't enough to ensure protection for your information assets. It's the people who make the difference in whether your security program is successful or just whitewash for auditors and investors. Involve your employees. Help them to see the importance of information security.

 Tom Olzak, MBA, CISSP, MCSE, is President and CEO of Erudio Security, LLC. He can be reached at tom.olzak@erudiosecurity.com. Additional security management resources are available at http://adventuresinsecurity.com. Visit our blog at http://blogs.ittoolbox.com/security/adventures/

Works Cited

Taylor, L. (2004, October). Security awareness and training 101. *Intranet Journal*. Retrieved April 4, 2006 from http://intranetjournal.com/articles/200410/pij_10_11_04a.html

Wilson, M. and Hash, J. (2003, October). *Building an information technology security awareness and training program (NIST SP 800-50).* Retrieved April 4, 2006 from http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf