ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

INFORMATION TECHNOLOGY SECURITY AWARENESS, TRAINING, EDUCATION, AND CERTIFICATION

By Mark Wilson and Joan Hash
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Introduction

Federal agencies and private sector organizations cannot protect the confidentiality, integrity, and availability of information in today's highly networked systems environment without ensuring that all people involved in using and managing information technology (IT):

- Understand their roles and responsibilities related to the organizational mission;
- Understand the organization's IT security policy, procedures, and practices; and
- Possess at least adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible.

As cited in audit reports, periodicals, and conference presentations, the IT security professional community understands that people are one of the weakest links in attempts to secure systems and networks. The *people factor* - not technology - is key to providing an adequate and appropriate level of security. If people are the key, but are also a weak link, more and better attention must be paid to this asset. A robust and enterprisewide awareness and training program is paramount to ensuring that people understand their IT security responsibilities, and properly use and protect the IT resources entrusted to them.

NIST Special Publication (SP) 800-50, *Building an Information Technology Security Awareness and Training Program*, by Mark Wilson and Joan Hash, provides guidelines that can help federal departments and agencies meet their security training responsibilities contained in the Federal Information Security Management Act (FISMA) and Office of Management and Budget (OMB) guidance. The document gives guidance for building and maintaining a comprehensive awareness and training program, as part of an organization's IT security program. This *ITL Bulletin* summarizes NIST SP 800-50, which is available at http://csrc.nist.gov/publications/nistpubs/index.html.

The document is a companion publication to NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* (also available at the above website). The two publications are complementary; SP 800-50 works at a higher strategic level, discussing how to build an IT security awareness and training program, while SP 800-16 addresses a more tactical level, describing an approach to role-based IT security training.

The agency IT security program policy should contain a clear and distinct section devoted to agencywide requirements for the awareness and training program. Topics documented within the awareness and training program policy should include roles and responsibilities, development of program strategy and a program plan, implementation of the program plan, and maintenance of the awareness and training program.

Components: Awareness, Training, Education, and Certification

A successful IT security program consists of:

- developing IT security policy that reflects business needs tempered by known risks;

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8901, Gaithersburg, MD 20899-8901, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since June 2002

- informing users of their IT security responsibilities (through awareness and training), as documented in agency security policy and procedures; and
- establishing processes for monitoring, reviewing, and updating the program.

An awareness and training program is crucial, in that it is *the* vehicle for disseminating information that users, including managers, need in order to do their jobs. In the case of an IT security program, it is *the* vehicle to be used to communicate security requirements across the enterprise.

An effective IT security awareness and training program explains proper rules of behavior for the use of agency IT systems and information. The program communicates IT security policies and procedures that need to be followed. This must precede and lay the basis for any sanctions imposed due to noncompliance. Through awareness and training, users first should be informed of the expectations. Accountability must be derived from a fully informed, well-trained, and aware workforce.

Awareness: Security awareness efforts are designed to change behavior or reinforce good security practices. Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance.

Training: Training strives to produce relevant and needed security skills and competencies. The most significant difference between training and awareness is that training seeks to teach skills that allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues.

Education: Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles (technological and social), and strives to produce IT security specialists and professionals capable of vision and proactive response.

Certification: Professional development is intended to ensure that users, from beginner to the career security professional, possess a required level of knowledge and competence necessary for their roles. Professional development validates skills through certification. Such development and successful certification can be termed "professionalization." The preparatory work to testing for such a certification normally includes study of a prescribed body of knowledge or technical curriculum, and may be supplemented by on-the-job experience.

The movement toward professionalization within the IT security field can be seen among IT security officers, IT security auditors, IT contractors, and system/network administrators and is evolving. There are two types of certification: general and technical. The general certification focuses on establishing a foundation of knowledge on the many aspects of the IT security profession. The technical certification focuses primarily on the technical security issues related to specific platforms, operating systems, vendor products, etc.

Some agencies and organizations focus on IT security professionals with certifications as part of their recruitment efforts. Other organizations offer pay raises and bonuses to retain employees with certifications and encourage others in the IT security field to seek certification.

Designing, Developing, and Implementing an Awareness and Training Program

The development of an IT security awareness and training program involves three major steps:

- designing the program (including the development of the IT security awareness and training program plan),
- developing the awareness and training material, and
- implementing the program.

Even a small amount of IT security awareness and training can go a long way toward improving the IT security posture of, and vigilance within, an organization.

Designing: Awareness and training programs must be designed with the organization mission in mind. The awareness and training program must support the business needs of the organization and be relevant to the organization's culture and IT architecture. The most successful programs are those that users feel are relevant to the subject matter and issues presented.

Designing an IT security awareness and training program answers the question "What is our plan for developing and implementing awareness and training opportunities that are compliant with existing directives?" In the design step of the program, the agency's awareness and training needs are identified, an effective agencywide awareness and training plan is developed, organizational buy-in is sought and secured, and priorities are established.

Developing: Once the awareness and training program has been designed, supporting material can be developed. Material should be developed with the following in mind:

- ***"What behavior do we want to reinforce?"*** (awareness); and
- ***"What skill or skills do we want the audience to learn and apply?"*** (training).

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

In both cases, the focus should be on specific material that the participants should integrate into their jobs. Attendees will pay attention and incorporate what they see or hear in a session if they feel that the material was developed specifically for them. Any presentation that feels canned – impersonal and so general as to apply to any audience – will be filed away as just another of the annual "we're here because we have to be here" sessions. An awareness and training program can be effective, however, if the material is interesting and current.

The awareness audience must include all users in an organization. Users may include employees, contractors, foreign or domestic guest researchers, other agency personnel, visitors, guests, and other collaborators or associates requiring access. The message to be spread through an awareness program, or campaign, should make all individuals aware of their commonly shared IT security responsibilities. On the other hand, the message in a training class is directed at a specific audience. The message in training material should include everything related to security that attendees need to know in order to perform their jobs. Training material is usually far more in-depth than material used in an awareness session or campaign.

Implementing: An IT security awareness and training program should be implemented only after a needs assessment has been conducted, a strategy has been developed, an awareness and training program plan for implementing that strategy has been completed, and awareness and training material has been developed.

The program's implementation must be fully explained to the organization to achieve support for its implementation and commitment of necessary resources. This explanation includes expectations of agency management and staff support, as well as expected results of the program and benefits to the organization. Funding issues must also be addressed. For example, agency managers must know if the cost to implement the awareness and training program will be totally funded by the Chief Information Officer (CIO) or IT security program budget, or if their budgets will be impacted to cover their share of the expense of implementing the program. It is essential that everyone involved in the implementation of the program understand their roles and responsibilities. In addition, schedules and completion requirements must be communicated.

Once the plan for implementing the awareness and training program has been explained to (and accepted by) agency management, the implementation can begin. A number of ways exist for awareness and training material to be presented and disseminated throughout an organization. Agencies should tailor their implementation to the size, organization, and complexity of their enterprise. See NIST SP 800-50, Section 5, for techniques for delivering awareness and training material.

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov/.

Post-Implementation

An organization's IT security awareness and training program can quickly become obsolete if sufficient attention is not paid to technology advancements, IT infrastructure and organizational changes, and shifts in organizational mission and priorities. CIOs and IT security program managers need to be cognizant of this potential problem and incorporate mechanisms into their strategy to ensure the program continues to be relevant and compliant with overall objectives. Continuous improvement should always be the theme for security awareness and training initiatives, as this is one area where "*you can never do enough*."

Monitoring Compliance: Once the program has been implemented, processes must be put in place to monitor compliance and effectiveness. An automated tracking system should be designed to capture key information regarding program activity (e.g., courses, dates, audience, costs, sources). The tracking system should capture this data at an agency level, so that it can be used to provide enterprisewide analysis and reporting regarding awareness, training, and education initiatives.

Tracking compliance involves assessing the status of the program as indicated by the database information and mapping it to standards established by the agency. Reports can be generated and used to identify gaps or problems. Corrective action and necessary follow-up can then be taken. This may take the form of formal reminders to management; additional awareness, training, or education offerings; and/or the establishment of a corrective plan with scheduled completion dates.

Evaluation and Feedback: Formal evaluation and feedback mechanisms are critical components of any security awareness, training, and education program. Continuous improvement cannot occur without a good sense of how the existing program is working. In addition, the feedback mechanism must be designed to address objectives initially established for the program. Once the baseline requirements have been solidified, a feedback strategy can be designed and implemented. Various evaluation and feedback mechanisms that can be used to update the awareness and training program plan include surveys, evaluation forms, independent observation, status reports, interviews, focus groups, technology shifts, and benchmarking.

A feedback strategy needs to incorporate elements that will address quality, scope, deployment method (e.g., web-based, onsite, offsite), level of difficulty, ease of use, duration of session, relevancy, currency, and suggestions for modification.

Managing Change: It will be necessary to ensure that the program, as structured, continues to be updated as new technology and associated security issues emerge. Training needs will shift as new skills and capabilities become necessary

to respond to new architectural and technology changes. A change in the organizational mission and/or objectives can also influence ideas regarding how best to design training venues and content. Emerging issues, such as homeland defense, will also impact the nature and extent of security awareness activities necessary to keep users informed/educated about the latest exploits and countermeasures. New laws and court decisions may also impact agency policy that, in turn, may affect the development and/or implementation of awareness and training material. Finally, as security directives change or are updated, awareness and training material should reflect these changes.

Program Success Indicators: CIOs, program officials, and IT security program managers should be primary advocates for continuous improvement and for supporting an agency's security awareness, training, and education program. It is critical that everyone be capable and willing to carry out their assigned security roles in the organization. In security, the phrase, *only as strong as the weakest link*, is true. Securing an organization's information and infrastructure is a *team* effort. Listed below are some key indicators to gauge the support for, and acceptance of, the program.

- Sufficient funding to implement the agreed-upon strategy.
- Appropriate organizational placement to enable those with key responsibilities (CIO, program officials, and IT security program manager) to effectively implement the strategy.
- Support for broad distribution (e.g., web, e-mail, TV) and posting of security awareness items.
- Executive/senior-level messages to staff regarding security (e.g., staff meetings, broadcasts to all users by agency head).
- Use of metrics (e.g., to indicate a decline in security incidents or violations, indicate that the gap between existing awareness and training coverage and identified needs is shrinking, the percentage of users being exposed to awareness material is increasing, the percentage of users with significant security responsibilities being appropriately trained is increasing).
- Managers do not use their status in the organization to avoid security controls that are consistently adhered to by the rank and file.
- Level of attendance at mandatory security forums/briefings.
- Recognition of security contributions (e.g., awards, contests).
- Motivation demonstrated by those playing key roles in managing/coordinating the security program.

Conclusion

Government and industry organizations must protect the confidentiality, integrity, and availability of information in today's highly networked systems environment. A robust IT security awareness and training program, as part of the overall IT security program, gives users the needed tools and information to protect an agency's vital information resources. Addressing the *people factor* is key to ensuring an adequate and appropriate level of IT security within an organization, large or small. We invite you to visit our Computer Security Resource Center at http://csrc.nist.gov for more information on a wide range of IT security topics.

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900

Official Business
Penalty for Private Use $300

Address Service Requested

PRSRT STD
POSTAGE & FEES PAID
NIST
PERMIT NUMBER G195