ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

TRAINING FOR INFORMATION TECHNOLOGY SECURITY: EVALUATING THE EFFECTIVENESS OF RESULTS-BASED LEARNING

The basic principles of results-based training for information technology (IT) security were discussed in our April 1998 bulletin, Training Requirements for Information Technology Security: An Introduction to Results-Based Learning. This learning approach trains staff members according to their roles and responsibilities within their organizations and recommends that organizations evaluate the results of the training. Both this bulletin and the April bulletin were excerpted from NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. The training requirements were developed by the Federal Computer Security Program Managers Forum and by the Federal Information Systems Security Educators' Association (FISSEA). The complete publication is available in paper copy from the Government Printing Office and in electronic format from NIST's Web pages:

http://csrc.nist.gov/training/800-16.pdf

The Role- and Performance-Based Model

Results-based training for information technology (IT) security focuses on the job functions that individuals perform, and on their specific roles and responsibilities within their organizations. The results-based approach to learning is based on the premise that individuals have unique backgrounds and different ways of learning. Another consideration is that individuals may have more than one role in the organization, and they may need information technology security training that is tailored for the specific responsibilities of each role.

The role- and performance-based model presented in NIST Special Publication 800-16 provides a systematic and integrated framework for identifying training needs throughout the organization and for ensuring that individuals receive the training that they need. The framework relates job function to the IT security knowledge that is required to carry out a specific job. Managers can then identify needed training for their staff members, understand the consequences of not providing adequate training, and plan and schedule training according to organizational priorities.

In the model, learning is represented as a continuum that starts with awareness, continues with training, and evolves into education. Awareness about IT security is the point-of-entry into the learning process for all employees. The next step is training, which starts with instruction on security basics and literacy, and then carries through with instruction in a wide

Continued on page 2

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 to listproc@nist.gov with the message **subscribe itl-bulletin**, and your proper 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.

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, Room 562, Building 820, Gaithersburg, MD 20899, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and address to this office.

Bulletins issued since August 1996:

- *Implementation Issues for Cryptography*, August 1996
- *Generally Accepted System Security Principles (GSSPs): Guidance On Securing Information Technology (IT) Systems*, October 1996
- *Federal Computer Incident Response Capability (FEDCIRC)*, November 1996
- *Security Issues for Telecommuting*, January 1997
- *Advanced Encryption Standard*, February 1997
- *Audit Trails*, March 1997
- *Security Considerations in Computer Support and Operations*, April 1997
- *Public Key Infrastructure Technology*, July 1997
- *Cryptography Standards and Supporting Infrastructures: A Status Report*, September 1997
- *Internet Electronic Mail*, November 1997
- *Information Security and the World Wide Web (WWW)*, February 1998
- *Management of Risks in Information Systems: Practices of Successful Organizations*, March 1998
- *Training Requirements for Information Technology Security: An Introduction to Results-Based Learning*, April 1998
- *A Comparison of Year 2000 Solutions*, May 1998

range of security-related skills needed by employees for their specific roles and responsibilities. The capstone of the learning continuum is education, which creates the expertise needed by the organization's IT security specialists and professionals.

The model is very useful in helping managers meet their responsibilities for training staff members. In addition, the model helps course developers identify the learning outcomes expected for individuals with various roles and responsibilities. As a result, IT security course material can be developed in basic modules and then appropriately customized to meet the needs of individual staff members.

Evaluating the Effectiveness of Training

Training based on organizational and staff members' needs is a good investment for the organization. But to receive the benefits, the organization must ensure that the contents of the training are current and appropriate for the audience, and that the training is delivered in an effective manner.

As part of their regular processes for the wise management of resources, organizations should evaluate the scope of their IT security training needs and the effectiveness of the training provided. Evaluations enable decision-makers to allocate their training resources sensibly and to derive the greatest return on their training investments. When training resources are well-managed, the organization benefits both from improved IT security and from stronger management support for the IT security activities.

The evaluation process starts with identifying what can be measured. Some aspects of training for which evaluation data can be collected include the following:

- The learner's satisfaction with the training - the extent to which the conditions were right for learning.
- Learning effectiveness - what an individual has learned from a specific course or training event.
- Teaching effectiveness – the pattern of learner outcomes following a specific course or training event.
- Program effectiveness - the value of the specific class or training event, compared to other options in the context of an organization's overall IT security training program.

The time and resources spent in conducting training evaluations can be beneficial to employees, managers, and trainers. Employees benefit by being able to assess their own post-training job performance. Managers can use the evaluations to assess the subsequent on-the-job performance of staff members. In addition, managers can use the evaluations to make decisions about how to allocate limited resources among the various IT security activities in the continuum from awareness, security literacy, and training to education. Another benefit is that trainers can use trend data acquired from evaluations to improve both their teaching and student learning.

Developing an Evaluation Plan

It is difficult to get good information for evaluating learner satisfaction and the effectiveness of training programs. Written learning objectives, stated in an observable, measurable way, are needed to evaluate student learning. To evaluate teaching, it is necessary to collect trend and other related data. Mission-related goals must be identified and related to learning objectives in order to evaluate returns on investment.

Before initiating evaluations, organizations should develop plans for gathering the evaluation information that they need. The following are suggested elements to be included when developing the evaluation plan:

- **A written description of existing conditions prior to, and in preparation for, the learning activity.** Certain conditions must be present to forecast training effectiveness. Does the student need a checklist, a set of items to manipulate, or an outline of the information? Does the instructor need audiovisual equipment, handouts, or a classroom with furniture set up in a specific format? Conditions of the learning activity, including computer-based training (CBT), must be specific and comprehensive.
- **The activity to be performed.** The evaluation plan must state the activity to be performed in a manner permitting the evaluator to actually observe the behavior that the student is to learn. Observations can be done in class by the teacher or on the job by the supervisor. It is very difficult and impractical to measure the process of a student's changing attitude or thinking through a task or problem. The evaluator, however, can measure a written exercise, a demonstration of skill, a verbal or written discussion, or any combination of these demonstrable activities. Rather than merely acknowledging that the student was exposed to certain information, the evaluator should observe the skill being performed or the information being applied. In computer-based training, evaluation measurement can be programmed to occur at the instructional unit level, with subsequent units adjusted based on student response. In other instructional methods, adjustments can be made in real time by the instructor based on the nature of student questions during the course. Adjustments can also be made between courses in a student's training sequence.
- **Measures of success derived from the individual's normal work products rather than from classroom testing**. This directly ties the individual's performance to the impact on the organization's mission. Written behavioral objectives for a learning activity must include a stated level of success. For example, quantitative skills can be expressed as being performed successfully every time, 10 out of 100 times, or 5 out of 10 times, and the impact or consequences can be noted. Risk management techniques should be used to establish the criticality of quantitative skills. Qualitative skills can be measured by distinguishing satisfactory performance from poor performance, or outstanding performance from

satisfactory performance. Measurements of qualitative skills might include the amount of repeat work required on the part of the learner, customer satisfaction, or peer recognition of the employee as a source of IT security information.

The nature and purpose of the training activity, and whether it is at a beginning, intermediate, or advanced level, will influence the setting of success measures. This is a subjective goal. If success levels are not documented, an individual student's achievement of the behavioral learning objectives cannot be evaluated, nor can the learning activity itself be evaluated as part of the organization's overall training program.

In addition to the written objectives suggested above, the evaluation plan should show how the data will be collected and used. This step will help to stimulate support for the cost and effort of the data collection.

The Levels of Evaluation

There are four levels of evaluation that progress from relatively simple to rather complex. These levels of evaluation are related to the four purposes of evaluation.

Level 1: End-of-Course Evaluations *(Student Satisfaction)*

A common term for this type of evaluation is "the 'Smiley Face' evaluation." For example, Likert Scale-type forms ask the student to check a range of options from "poor" to "excellent" indicating the student's feelings about the training activity. The responses indicate the perceptions of the student and provide information about the conditions for learning. At this level of evaluation, questions could be asked about the student's satisfaction with the training facility and instructor, the manner of presentation of the content, and whether or not course objectives met the student's expectations. Although this type of evaluation does not provide in-depth data, it does provide rapid feedback from the learner's perspective.

Measurement of training effectiveness depends on an understanding of the background and skill levels of the people being trained. For example, technical training provided to a group of systems analysts and programmers will have a different level of effect than the same information provided to a group of accountants. Basic demographic data may be collected at the beginning or conclusion of the course. Information about the learners' satisfaction with the course and course material should be collected at the end of the course.

Level 2: Behavior Objective Testing *(Learning and Teaching Effectiveness)*

This level of evaluation measures how much information or the level of skill that was transmitted to the student participating in the training activity. The evaluation could be in various formats relative to the level of training. Participants in an IT security basic and literacy course could be given tests both before and after the course. At an intermediate or advanced training level, participants could be given a performance test, such as a case study to analyze. At the education level, essay questions exploring concepts would be appropriate. The evaluation format must relate to the behavioral objectives of the learning activity. This, in turn, drives the content being presented. The Level 2 evaluation provides instant feedback and is more objective than a Level 1 evaluation. Behavior objective testing assesses how much the student remembered or measures skills demonstrated by the student's performance at the end of the program. Level 2 evaluations can be built into each unit of instruction as the course progresses.

A Level 2 evaluation measures success in the transfer of information and skills to the student. It enables the evaluator to determine if a given student needs to repeat the course or attend a different type of learning activity that presents the same material in a different format. The evaluator should be able to see if a pattern of transfer problems exists and to determine whether or not the course itself may need to be revised or dropped from an organization's training program.

Behavior objective testing is possibly the most difficult measurement area to address. It is relatively easy to test the knowledge level of the attendees after completing a course or unit of instruction but it is not easy to determine when that learning took place. An attendee may have had knowledge of the subject area before receiving the instruction and participation in the course may have had little or no impact in expanding knowledge. As a result, information collected solely at the conclusion of a course or instructional unit must be examined with respect to the attendee's background and education.

An approach to determining the learning impact of a specific course or instructional unit is to test at the outset of the training and at the conclusion of the training and to compare the results. At the beginning and intermediate levels, it is appropriate to test a student's knowledge of a particular subject area by including questions or tasks where there is only a single right answer or approach. Questions regarding selection of the "best" answer among possible options should be reserved for those training environments where there is opportunity for

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.

analyzing why a particular answer is better than other answers.

Level 3: Job Transfer Skills
(Student Performance Effectiveness)

This evaluation is the first level that asks for more than student input. At this level, the evaluator, through a structured questionnaire usually administered 30 to 60 days following the training activity, asks the supervisor about the performance of the employee relative to the behavioral objectives of the course. This is a "before" and "after" job skills comparison. In some cases this information is difficult to obtain, especially when employees' job functions and grade levels permit them considerable autonomy, without direct supervision. Developing a valid questionnaire can be a challenge when supervisors observe only the result of employee actions. Nevertheless, a Level 3 evaluation, when it is successfully done, should begin to show the extent to which the learning activity benefits the organization as well as the employee.

Level 4: Organizational Benefit
(Training Program Effectiveness)

Level 4 evaluations can be difficult to undertake and hard to quantify. Among the possible approaches are structured, follow-up interviews with students, their supervisors, and colleagues. Another possible approach is comparison by a subject-matter expert of outputs produced by a student both before and after training. Still another approach could be some form of benchmarking or evaluation of the particular training activity in relation to other options for a particular job performance measure. In all cases, these evaluations involve quantifying the value of resultant improvement relative to the cost of training.

Level 4 evaluations can help senior managers answer questions about the most cost-effective way to spend limited training resources. For example, it may be more beneficial for the organization to focus resources on the education of a single, newly appointed IT security specialist rather than to train all employees in security basics and literacy. Or perhaps there might be a better return on investment to train 'front-end' systems designers and developers in building security rules commensurate with the sensitivity of the system, rather than train 'back-end' users in compliance with currently existing system rules. Determination of the purpose and objectives of a Level 4 evaluation, as well as the number of variables and the method of measurement of skill level, should be done following the completion of Level 3 evaluations and after a thorough review of the findings.

Summary

NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, provides detailed, specific information to help organizations in starting a comprehensive evaluation of their IT security training programs. Organizations should measure the effectiveness of their IT security training programs and the extent to which the programs are useful to the organization and are wise expenditures of training resources.

Evaluations of IT security training must start with planning for the collection of evaluation data. Evaluations should take place at many levels and should include the views of the students for each learning activity. Supervisors should be asked their views on the effectiveness of training, and the organization should provide views on the returns on investment. The evaluation process will result in the collection of both quantitative and qualitative data. Some of the data must be collected over an extended period of time. Organizations must commit time and attention to the analysis of the collected data in order to fully review the costs and benefits of IT security training programs and to make wise decisions in the expenditure of training resources.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Building 820/562
Gaithersburg, MD 20899

Official Business
Penalty for Private Use $300

Address Service Requested

BULK RATE
POSTAGE & FEES
PAID
NIST
PERMIT NUMBER G195