2. Components: Awareness, Training, Education

A successful IT security program consists of: 1) developing IT security policy that reflects business needs tempered by known risks; 2) informing users of their IT security responsibilities, as documented in agency security policy and procedures; and 3) establishing processes for monitoring and reviewing the program.[6]

Security awareness and training should be focused on the organization's entire user population. Management should set the example for proper IT security behavior within an organization. An awareness program should begin with an effort that can be deployed and implemented in various ways and is aimed at all levels of the organization including senior and executive managers. The effectiveness of this effort will usually determine the effectiveness of the awareness and training program. This is also true for a successful IT security 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. Users first should be informed of the expectations. Accountability must be derived from a fully informed, well-trained, and aware workforce.

This section describes the relationship between awareness, training, and education – the awareness-training-education continuum.

2.1 The Continuum

Learning is a continuum; it starts with awareness, builds to training, and evolves into education. The continuum is illustrated in Figure 2-1. The continuum is further described in Chapter 2 of NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model,* available at http://csrc.nist.gov/publications/nistpubs/index.html.[7]

[6] An effective IT security awareness and training program can succeed only if the material used in the program is firmly based on agency IT security program policy and IT issue-specific policies. If policies are written clearly and concisely, then the awareness and training material – based on the policies – will be built on a firm foundation.

[7] The continuum is mentioned here and shown in Figure 2-1 to show the conceptual relationship between awareness, training, and education as described in NIST Special Publication 800-16. For the purposes of this guideline, clear boundaries are established between the three methods of learning.

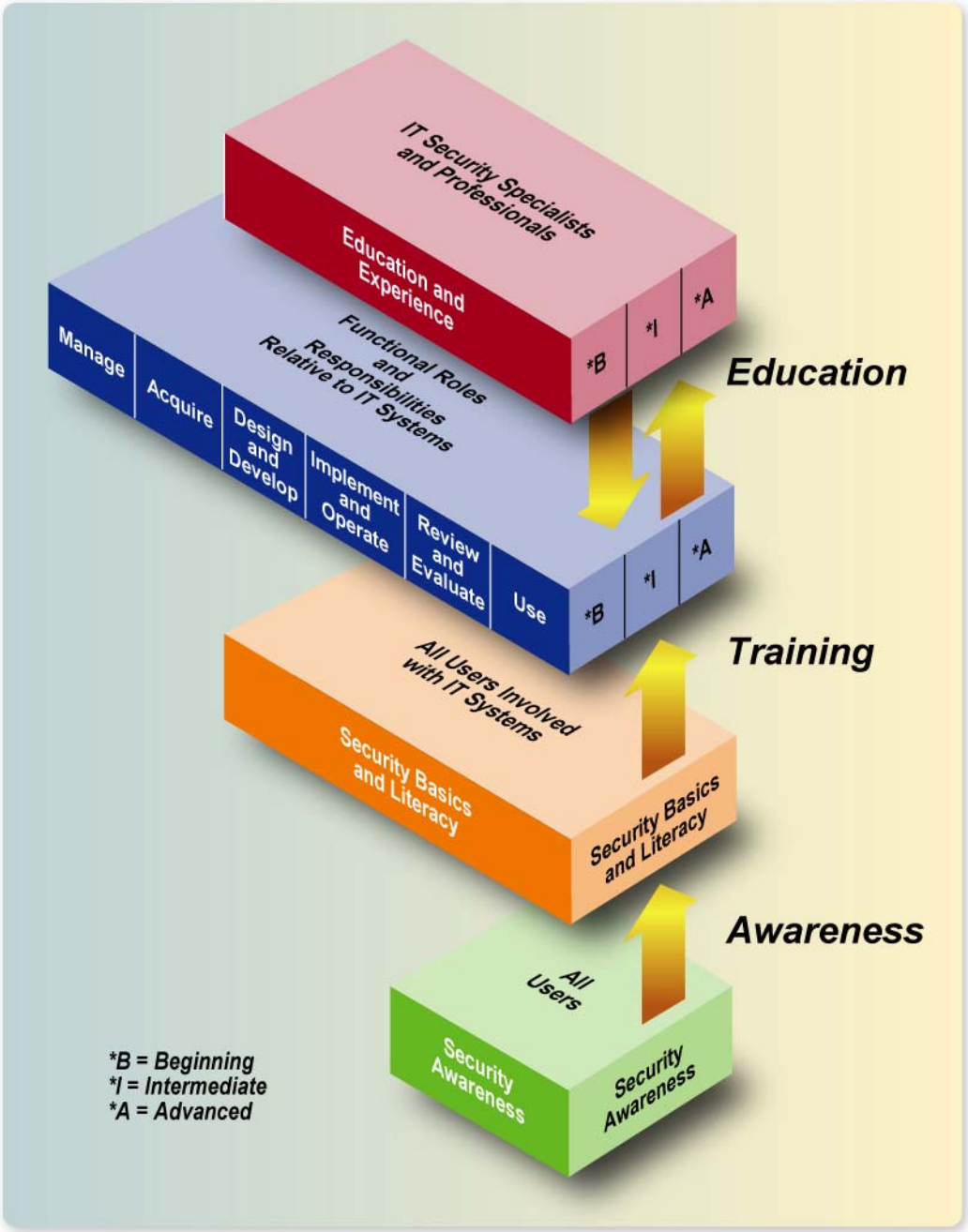

Figure 2-1: The IT Security Learning Continuum

2.2 Awareness

Security awareness efforts are designed to change behavior or reinforce good security practices. Awareness is defined in NIST Special Publication 800-16 as follows: *"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 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.

In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. 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."

An example of a topic for an awareness session (or awareness material to be distributed) is virus protection. The subject can simply and briefly be addressed by describing what a virus is, what can happen if a virus infects a user's system, what the user should do to protect the system, and what the user should do if a virus is discovered. A list of possible awareness topics can be found in Section 4.1.1.

A bridge or transitional stage between awareness and training consists of what NIST Special Publication 800-16 calls *Security Basics and Literacy*. The basics and literacy material is a core set of terms, topics, and concepts. Once an organization has established a program that increases the general level of security awareness and vigilance, the basics and literacy material allow for the development or evolution of a more robust awareness program. It can also provide the foundation for the training program.

2.3 Training

Training strives to produce relevant and needed security skills and competencies.

Training is defined in NIST Special Publication 800-16 as follows: "The 'Training' level of the learning continuum strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security (e.g., management, systems design and development, acquisition, auditing)." The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues. The skills acquired during training are built upon the awareness foundation, in particular, upon the security basics and literacy material. A training curriculum must not necessarily lead to a formal degree from an institution of higher learning; however, a training course may contain much of the same material found in a course that a college or university includes in a certificate or degree program.

An example of training is an IT security course for system administrators, which should address in detail the management controls, operational controls, and technical controls that should be implemented. Management controls include policy, IT security program management, risk management, and life-cycle security. Operational controls include personnel and user issues, contingency planning, incident handling, awareness and training, computer support and operations, and physical and environmental security issues. Technical controls include identification and authentication, logical access controls, audit trails, and cryptography. (See NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, for in-depth discussion of these controls (http://csrc.nist.gov/publications/nistpubs/index.html).)

2.4 Education

Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge . . . and strives to produce IT security specialists and professionals capable of vision and pro-active response.

Education is defined in NIST Special Publication 800-16 as follows: *"The 'Education' level 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 pro-active response."*

An example of education is a degree program at a college or university. Some people take a course or several courses to develop or enhance their skills in a particular discipline. This is training as opposed to education. Many colleges and universities offer certificate programs, wherein a student may take two, six, or eight classes, for example, in a related discipline, and is awarded a certificate upon completion. Often, these certificate programs are conducted as a joint effort between schools and software or hardware vendors. These programs are more characteristic of training than education. Those responsible for security training need to assess both types of programs and decide which one better addresses identified needs.

2.5 Professional Development

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 users with certifications and encourage others in the IT security field to seek certification.

3. Designing an Awareness and Training Program

There are three major steps in the development of an IT security awareness and training program – 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. This section describes the first step in the development of an awareness and training program: designing the program.

Awareness and training programs must be designed with the organization mission in mind. It is important that the awareness and training program supports 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?"[8] In the design step of the program, the agency's awareness and training needs are identified, an effective agency wide awareness and training plan is developed, organizational buy-in is sought and secured, and priorities[9] are established.

This section describes:

- How to structure the awareness and training activity;
- How to (and why) conduct a needs assessment;
- How to develop an awareness and training plan;
- How to establish priorities;
- How to "set the bar" (i.e., the level of complexity of the subject matter) properly; and
- How to fund the awareness and training program.

3.1 Structuring an Agency Awareness and Training Program

An awareness and training program may be designed, developed, and implemented in many different ways. Three common approaches or models are described below:

- Model 1: Centralized policy, strategy, and implementation;
- Model 2: Centralized policy and strategy, distributed implementation; and
- Model 3: Centralized policy, distributed strategy and implementation.

The model that is embraced and established to oversee the awareness and training program activity depends on:

- The size and geographic dispersion of the organization;

[8] The awareness and training plan should reflect the organization's strategy for meeting its awareness and training program responsibilities.

[9] Priorities include what awareness or training material will be developed first and who will be the first to receive the material.

- Defined organizational roles and responsibilities; and
- Budget allocations and authority.

Model 1: Centralized Program Management Model (Centralized Policy, Strategy, and Implementation)

In this model, responsibility and budget for the entire organization's IT security awareness and training program is given to a central authority. All directives, strategy development, planning, and scheduling is coordinated through this "security awareness and training" authority.

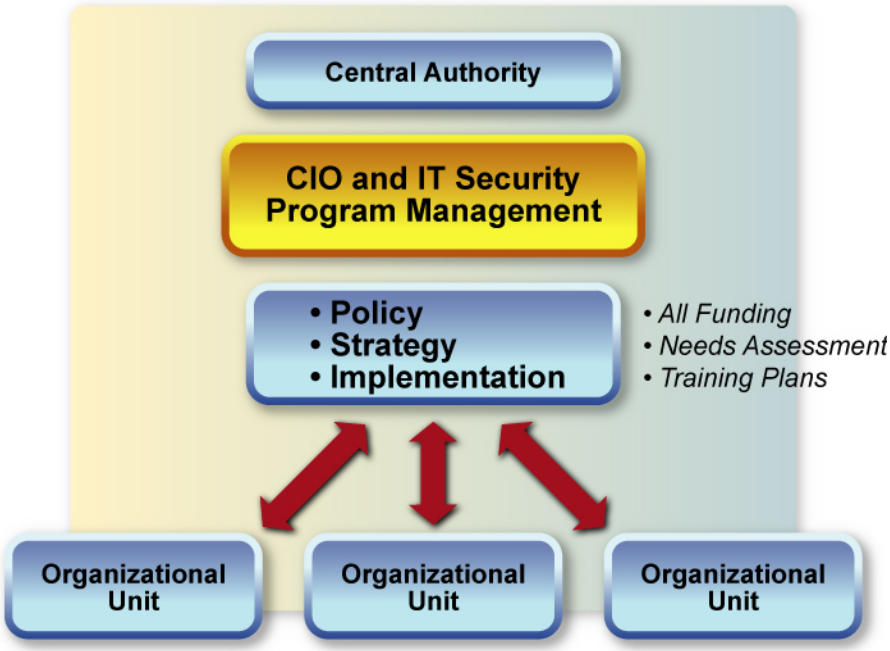

Figure 3-1: Model 1 – Centralized Program Management

Because the awareness and training strategy is developed at the central authority, the needs assessment – which helps determine the strategy – is also conducted by the central authority. The central authority also develops the training plan as well as the awareness and training material. The method(s) of implementing the material throughout the organization is determined and accomplished by the central authority. Typically, in such an organization, both the CIO and IT security program manager are organizationally located within this central authority.

Communication between the central authority and the organizational units travels in both directions. The central authority communicates the agency's policy directives regarding IT security awareness and training, the strategy for conducting the program, and the material and method(s) of implementation to the organizational units. The organizational units provide information requested by the central authority. For example, to meet its responsibilities, the central authority may collect data on the number of attendees at awareness sessions, the number of people trained on a particular topic, and the number of people yet to attend awareness and training sessions. The organizational unit can also provide feedback on the effectiveness of awareness and training material and on the appropriateness of the method(s) used to implement the material. This allows the central authority to fine-tune, add or delete material, or modify the implementation method(s).

This centralized program management model is often deployed by agencies that:

- Are relatively small or have a high degree of structure and central management of most IT functions;
- Have, at the headquarters level, the necessary resources, expertise, and knowledge of the mission(s) and operations at the unit level; or
- Have a high degree of similarity in mission and operational objectives across all of its components.

Model 2: Partially Decentralized Program Management Model (Centralized Policy and Strategy; Distributed Implementation)

In this model, security awareness and training policy and strategy are defined by a central authority, but implementation is delegated to line management officials in the organization. Awareness and training budget allocation, material development, and scheduling are the responsibilities of these officials.

The needs assessment is conducted by the central authority, because they still determine the strategy for the awareness and training program. Policy, strategy, and budget are passed from the central authority to the organizational units. Based on the strategy, the organizational units develop their own training plans. The organizational units develop their awareness and training material, and determine the method(s) of deploying the material within their own units.

As was the case in the centralized program management model (Model 1), communication between the central authority and the organizational units travels in both directions in this model. The central authority communicates the agency's policy directives regarding IT security awareness and training, the strategy for conducting the program, and the budget for each organizational unit. The central authority may also advise the organizational units that they are responsible for developing training plans and for implementing the program, and may provide guidance or training to the organizational units so that they can carry out their responsibilities.

The central authority may require periodic input from each organizational unit, reporting the budget expenditures made, the status of unit training plans, and progress reports on the implementation of the awareness and training material. The central authority may also require the organizational units to report the number of attendees at awareness sessions, the number of people trained on a particular topic, and the number of people yet to attend awareness and training sessions. The organizational unit may be asked to describe lessons learned, so the central authority can provide effective guidance to other units.

Figure 3-2: Model 2 - Partially Decentralized Program Management

This partially decentralized program management model is often deployed by agencies that:

- Are relatively large or have a fairly decentralized structure with clear responsibilities assigned to both the headquarters (central) and unit levels;
- Have functions that are spread over a wide geographical area; or
- Have organizational units with diverse missions, so that awareness and training programs may differ significantly, based on unit-specific needs.

Model 3: Fully Decentralized Program Management Model (Centralized Policy; Distributed Strategy and Implementation)

In this model, the central security awareness and training authority (CIO/IT security program manager) disseminates broad policy and expectations regarding security awareness and training requirements, but gives responsibility for executing the entire program to other organizational units. This model normally uses a series of *distributed authority* directives, driven from the central authority. This normally means creation of a subsystem of CIOs and IT security program managers subordinate to the central CIO and IT security officer.

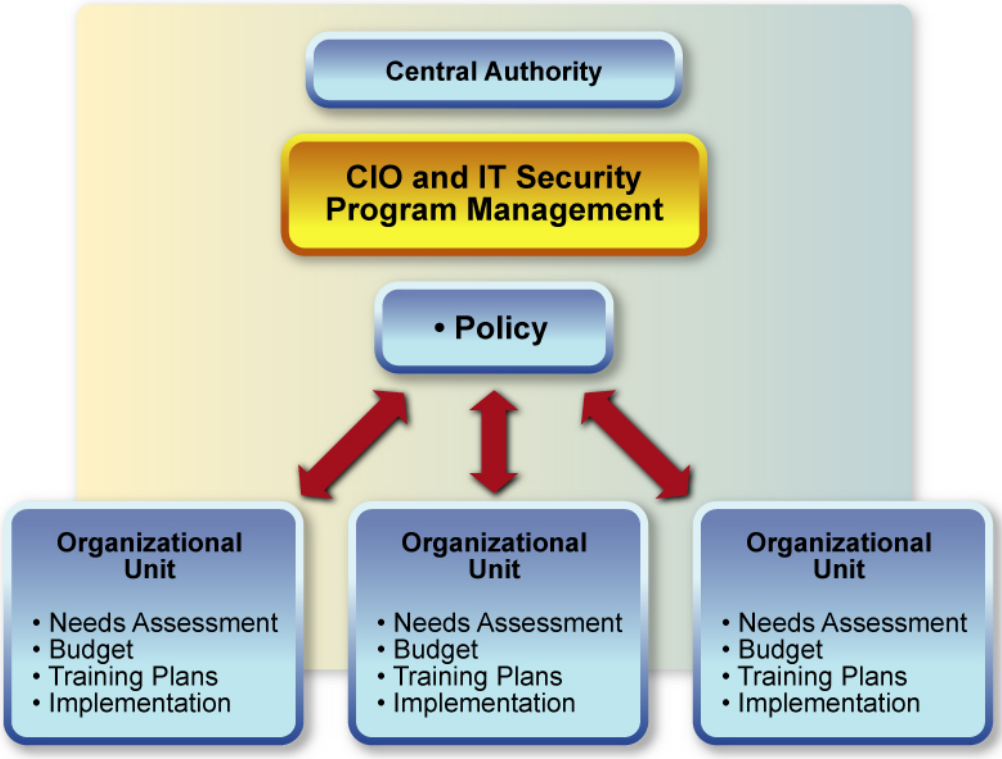

Figure 3-3: Model 3 – Fully Decentralized Program Management

The needs assessment is conducted by each organizational unit, because in this model, the units determine the strategy for the awareness and training program. Policy and budget are passed from the central authority to the organizational units. Based on the strategy, the organizational units develop their own training plans. The organizational units develop their awareness and training material, and determine the method(s) of deploying the material within their own units.

As was the case in the centralized program management model (Model 1) and the partially decentralized program management model (Model 2), communication between the central authority and the organizational units travels in both directions in this model. The central authority communicates the agency's policy directives regarding IT security awareness and training, and the budget for each organizational unit. The central authority may also advise the organizational units that they are responsible for conducting their own needs assessment, developing their strategy, developing training plans, and implementing the program. The central authority may provide guidance or training to the organizational units so that they can carry out their responsibilities.

> Unless the central authority has a very good strategy for policy and program requirement enforcement and can take into account performance and operational issues at the unit level, utilizing the fully decentralized program management model may be "throwing the IT security program over the wall" with little or no accountability.

The central authority may require periodic input from each organizational unit, reporting the budget expenditures made, the status and results of needs assessments, the strategy chosen by the organizational unit, the status of training plans, and progress reports on the implementation of the awareness and training material. The central authority may also require the organizational units to report

the number of attendees at awareness sessions, the number of people trained on a particular topic, and the number of people yet to attend awareness and training sessions.

This fully decentralized program management model is often deployed by agencies that:

- Are relatively large;
- Have a very decentralized structure with general responsibilities assigned to the headquarters (central) and specific responsibilities assigned to unit levels;
- Have functions that are spread over a wide geographical area; or
- Have *quasi-autonomous* organizational units with separate and distinct missions, so that awareness and training programs may need to differ greatly.

Once the model to be employed is identified, the approach to conducting a needs assessment should be defined consistent with the organizational model selected.

3.2 Conducting a Needs Assessment

A needs assessment is a process that can be used to determine an organization's awareness and training needs. The results of a needs assessment can provide justification to convince management to allocate adequate resources to meet the identified awareness and training needs.

In conducting a needs assessment, it is important that key personnel be involved. As a minimum, the following roles should be addressed in terms of any special training needs:

- Executive Management – Organizational leaders need to fully understand directives and laws that form the basis for the security program. They also need to comprehend their leadership roles in ensuring full compliance by users within their units.
- Security Personnel (security program managers and security officers) – These individuals act as expert consultants for their organization and therefore must be well educated on security policy and accepted best practices.
- System Owners – Owners must have a broad understanding of security policy and a high degree of understanding regarding security controls and requirements applicable to the systems they manage.
- System Administrators and IT Support Personnel – Entrusted with a high degree of authority over support operations critical to a successful security program, these individuals need a higher degree of technical knowledge in effective security practices and implementation.
- Operational Managers and System Users – These individuals need a high degree of security awareness and training on security controls and rules of behavior for systems they use to conduct business operations.

A variety of sources of information in an agency can be used to determine IT security awareness and training needs, and there are different ways to collect that information. Figure 3-4 suggests techniques for gathering information as part of a needs assessment.[10]

[10] The needs assessment process should only be as complex as is needed to identify an organization's awareness and training program needs. Similarly, the tools that are employed to identify those needs should be selected with an understanding of the organization's culture and conventions, as well as knowledge of the organization's size, workforce complexity, and