Role of Awareness and Training for Successful Information Systems Security Program

Venkata Siva,

Jose R Velez

Saint Leo University

Abstract

People are the most important asset of any organization at the same time they the weakest element in securing information systems and networks. Organizations usually give importance to technology instead of people who are the most critical factors in ensuring information systems security. The weakest link can become strong by creating awareness and training program to people within the organization. Success in protecting information systems can be achieved by continuously training in organizational security policies and responsibilities while protecting information systems. The project paper discusses the policy components and how to design, develop, implement, post-implementation issues, monitoring compliance, evaluation, feedback of the awareness and training program. With understanding keywords such as *Information Security, People, Awareness, and Training,* organizations can overcome security obstacles.

Role of Awareness and Training for Successful Information Systems Security Program

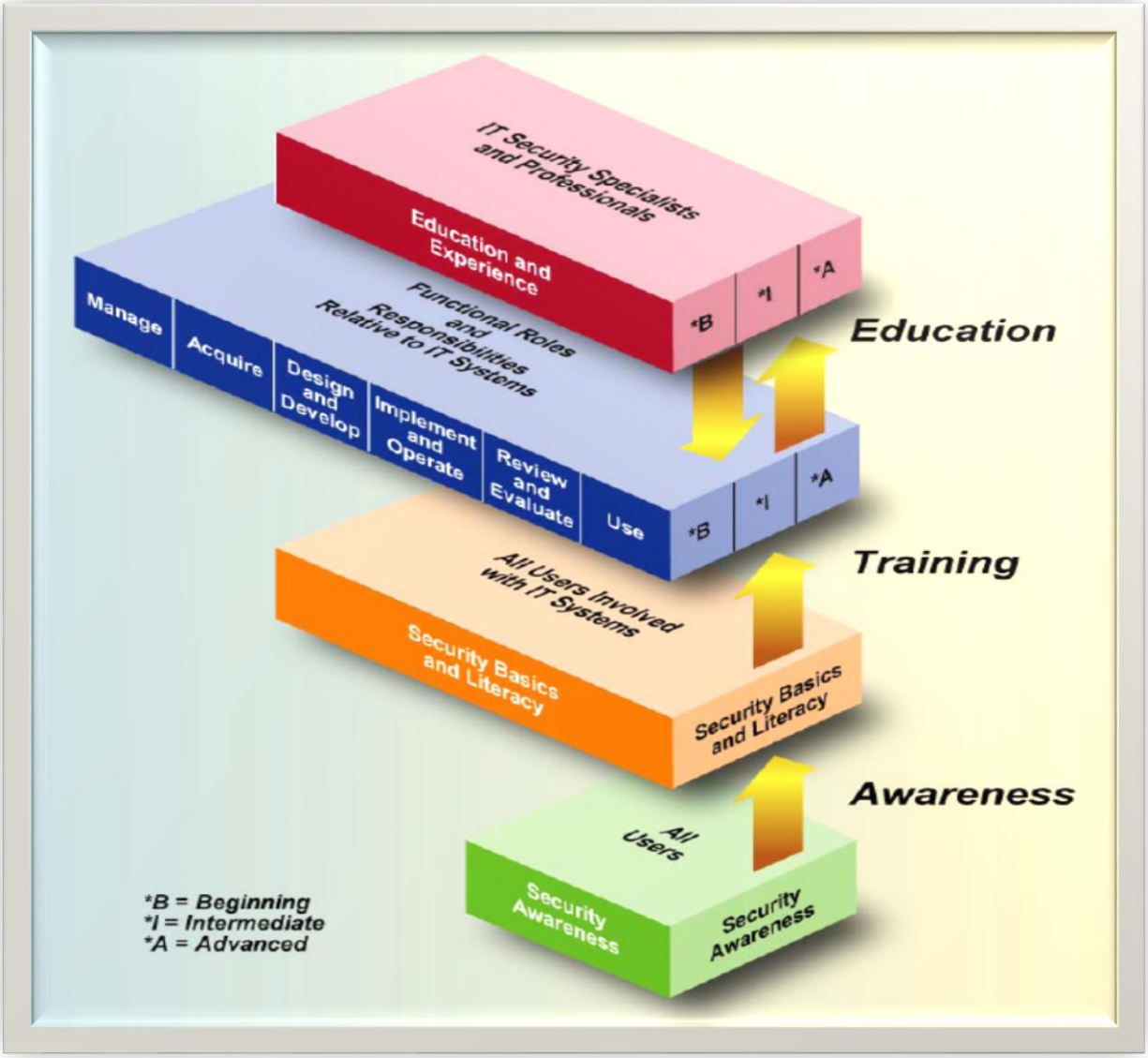
We want in this project paper briefly provide guidelines for information systems security, awareness, training, and education responsibilities. To define these security concepts, we have sourced some of the United States federal agencies like the Office of Personnel Management (OPM); the Nationals Institute of Standards and Technology (NIST); and the Office of Management and Budget (OBM). Also, we have cited the Federal Information Security Management Act (FISMA) to describe a better understand of the process of security awareness, training, and education programs. These bodies have highly stressed the importance on conducting awareness activities and role-based training as main security controls, which can ensure minimizing people risk, who are responsible for following procedures while managing, operating, and maintaining information systems and networks. This program gives security information required to follow when executing their jobs. Organizations must ensure its personnel understands the importance of achieving its security goals with the help of provided training. We realized that the success of Information Systems security is a team effort and all capable individual part of this team must carry out their assigned security roles within the organization.

The security awareness and training are being critical component of as a very important role; as well as one of the important component of Information security program. To achieve total security solution, the awareness and training program for workforce, plays an important role in achieving organization overall information security goals. The goal can be achieved only when all levels of workforce actively participate in the program. Organizations that continually train their workforce on policies and role-based security responsibilities; they will have higher success rate in protecting organization information assets. It has been proven time, and again,

that people are the weakest element in securing organization system and network security. Therefore, It is high time to realize that people is an important factor in security instead of technology. This equation has been noted in many security conferences such as the Annual Computer Security Application Conference (Los Angeles, California), and the Annual Conference for Cybersecurity at Florida USF. Briefly, let's introduce what is one of the rolls of the National Institute of Standards and Technology (NIST).

Realizing this, Federal Information Security Management Act (FISMA) and the office of Personnel Management (OPM) have mandated that organizations must devote resources to create awareness and role-based training. They stress as the people who use, manage, operate, and maintain information systems and networks. To acknowledge this, the National Institute of Standards and Technology (NIST) highlighted these guidelines in its publication (Building an Information Technology Security Awareness and Training Program , 2003). NIST is responsible for developing standards and guidelines, including minimum requirements, and for proving adequate information security for all agency operations and assets, but such standards and guide lines shall not apply for national security systems (Information Security Hand Book: A Guide for Managers NIT 800-50). Furthermore, NITS can help federal departments and agencies to meet their information security awareness and training responsibilities. In addition, these standards are in consistent with the requirements defined by the Federal Information Security Management Act (FISMA) and the Office of Management and Budget (OBM) policy (Information Security Handbook: A Guide for Managers NITS 800-100) The publication gave models for building and maintain a comprehensive awareness and training program as part of an organizations information security program. In other words, the NIST SP 800-50 works at a higher strategic level and discusses how to build and maintain an information security awareness and training

program; whereas, NIST SP 800-100 addresses a more tactical level and discusses the awareness-training-education continuum, role-based training, and course content considerations. To illustrate how these models – NIST 800-100 & NIST 800-50 – can work let's see the IT



Security Learning Continuum in the next graphic description:

Figure 1: IT security Learning Continuum (Source: NITS SP 800-100 & 50)

Awareness and Security Training Policy

FISMA apart from mandating organizations to implement training and awareness program OPM mandates organizations to identify and train senior management to create information security policy. OPM mandates organization to conduct awareness and training "At least annually" and role-based training in accordance with NIST guidance.

Enterprise-level policy and should include:

- Definition of security roles and responsibilities;
- Development of program strategy and a program plan;
- Implementation of the program plan; and
- Maintenance of the security awareness and training program.

The policy must contain clear and distinct section devoted to organization wide requirements for the awareness and training program.

Awareness

Security awareness solution consists of activities that promote security, establish accountability, and inform the workforce on latest security developments. Awareness should focus to get maximum attention of workforce on issues or a set of issues. Workforce needs to be pushed continuously to be aware of security policies in different formats. An awareness program includes tools, communication and metrics development.

Tools

Workforce must be made to realize "what" but not "how" of security program, and made aware of what in and what is not allowed as part of security program. Any disciplinary actions imposed if policies are not followed. Awareness also focus on the expected behavior of workforce while using organization information systems assets. The organizations must let

workforce know the acceptable level of expectations when using information systems. The tools can be organizing events like security awareness day, briefings on system or issue-specific along with promotional materials.

Communication.

Large part of awareness program goes in communicating policies among workforce from all levels. Communication plan need to identify stakeholders, type and frequency of security information exchanges. The direction (one or two way) of communication is also defined.

Training.

The main objective of information security program is to strive towards achieving knowledgeable and skilled workforce. Training helps workforce to enhance competency and learn how to implement their security role. Training helps in teaching skills to perform specific function while awareness seeks to focus an individual's attention on an issue or a set of issues. Training should be tailored to specific role-based groups or individual users who have significant responsibility handling information security in the organization. NIST provides role and performance based training programs.

Designing, Developing, and Implementing an Awareness and Training Program

Information security program is develop in main steps, Designing the program which includes information security awareness and training program plan, creating awareness and training material and implementing the actual program.

Designing an Awareness and Training Program

Organization mission must be considered while designing awareness and training program. The organization business needs, culture and information technology architecture are three main aspects to be considered while designing information system security program. Large

part of success depends on making users relevant part of the program. The program designing must answer an important question “is this program complaint to the existing directives?” in designing we have to identify the needs, plan is developed, top management buy-in is sought and secured, and priorities are established.

Developing an Awareness and Training Program

Once program design is completed the program supporting material can be developed. Material development must address questions “What behavior do we want to reinforce?” (Awareness) and “What skill or skills do we want the audience to learn and apply?” (Training). In both scenarios focus must be to develop materials relevant to their job function. We can get more attention if material developed specifically for them. Training will become interesting if the material is current, interesting and relevant.

Implementing an Awareness and Training Program

Once organization training and awareness needs are identified, strategy and material has been developed, the next step is to implement the information security program. The implementation plan must be fully explained to the stakeholders to get commitment and necessary resources, the cost of implementation, and budget allocations. Concerned parties involved must understand their roles and responsibilities. Schedule completion dates must be communicated as well. Once this implementation plan has been explained to the management, the implementation plan begins execution. Depending on the organization size, and complexity of their enterprise implementers can use several ways to present and disseminate awareness and training program throughout the organization.

Post-Implementation

Rapid technology advancements, IT infrastructure changes, organizational changes, and shifts in organizational mission and priorities can make program obsolete. CISO and senior management must be aware of these potential problem and develop strategies to counter them and ensure the program is current, relevant, and meets organization overall objectives. Continuous improvement must always be the theme for security awareness and training initiatives. Organization overall ongoing performance measures program has to be considered while gathering post-implementation feedback.

Monitoring Compliance

Once program has been implemented process must be put in place to monitor compliance and effectiveness. An automated tracking system has to be designed to capture key information on program activity. Tracking the status of the program compared to standards established by the organization. Any gaps or problems should be addressed based on the generate reports. These reports can help in taking corrective action and necessary follow-ups. The follow-up may be in the form of reminders to management, additional awareness and training programs and/or the establishment of a corrective plan with scheduled completion dates.

Evaluation and Feedback

Evaluation and Feedback mechanisms are critical components of any security awareness and training program. Good understanding of current programs performance will help continuous improvement of the 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/or benchmarking. A feedback strategy should incorporate elements that address quality, scope, deployment method (e.g., Web-based, onsite, offsite), and level of difficulty, ease of use, duration of session, relevancy, currency, and suggestions for modification.

Metrics are essential to feedback and evaluation. They can be used to:

- Measure the effectiveness of the security awareness and training program;
- Provide information for many of the data requests that an agency must provide with regard to compliance; and,
- Provide an important gauge for demonstrating progress and identifying areas for improvement.

CISO and top level management should be the advocates of awareness, training, and education. Organizations dedicated and capable individuals should work as a team while carrying out their assigned security roles. Some of the key indicators to measure, support and acceptance of organization awareness and training efforts:

- Sufficient funding is budgeted and available to implement the agreed-upon awareness and training strategy;
- Appropriate organizational placement of senior officials with key security responsibilities (CIO, program officials, and SAISO) facilitates strategy implementation;
- Infrastructure to support broad distribution (e.g., Web, e-mail, learning management systems) and posting of security awareness and training materials is funded and implemented;

- Executive/senior-level officials deliver messages to staff regarding security (e.g., staff meetings, broadcasts to all users by agency head), champion the program, and demonstrate support for training by committing financial resources to the program;
- Metrics indicate improved security performance by the workforce (e.g., to explain 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);
- Executives and 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 security forums/briefings/training is consistently high.
- Recognition of security contributions (e.g., awards, contests) is a standard practice within an agency; and
- Individuals playing key roles in managing/coordinating the security program demonstrate commitment to the program and motivation to promote the program.

References

Hash, M. W. (2003, 10). Building an Information Technology Security Awareness and Training Program . Gaithersburg, MD, USA.

Last Name, F. M. (Year). Article Title. *Journal Title*, Pages From - To.

Last Name, F. M. (Year). *Book Title.* City Name: Publisher Name.

Michael E. Whitman, H. J. (2013). *Management of Information Security, 3rd ED.* Boston, MA: Cengage Learning.

Pauline Bowen, J. H. (2006, 10). Information Security Hand Book: A Guide for Managers. Washingtong D.C., VA, USA.

Pauline Bowen, J. H. (2006, 10). Information Security Hand Book: A Guide for Managers NIT 800-50. Washingtong D.C., VA, USA.

Pauline Bowen, J. H. (2006, 10). Information Security Handbook: A Guide for Managers NITS 800-100. Washingtong D.C., VA, USA.

Security, D. o. (2015, October 18). *Department of Homeland Security*. Retrieved from Department of Homeland Security: http://www.dhs.gov/fisma