THEME 2

Systems of informational security

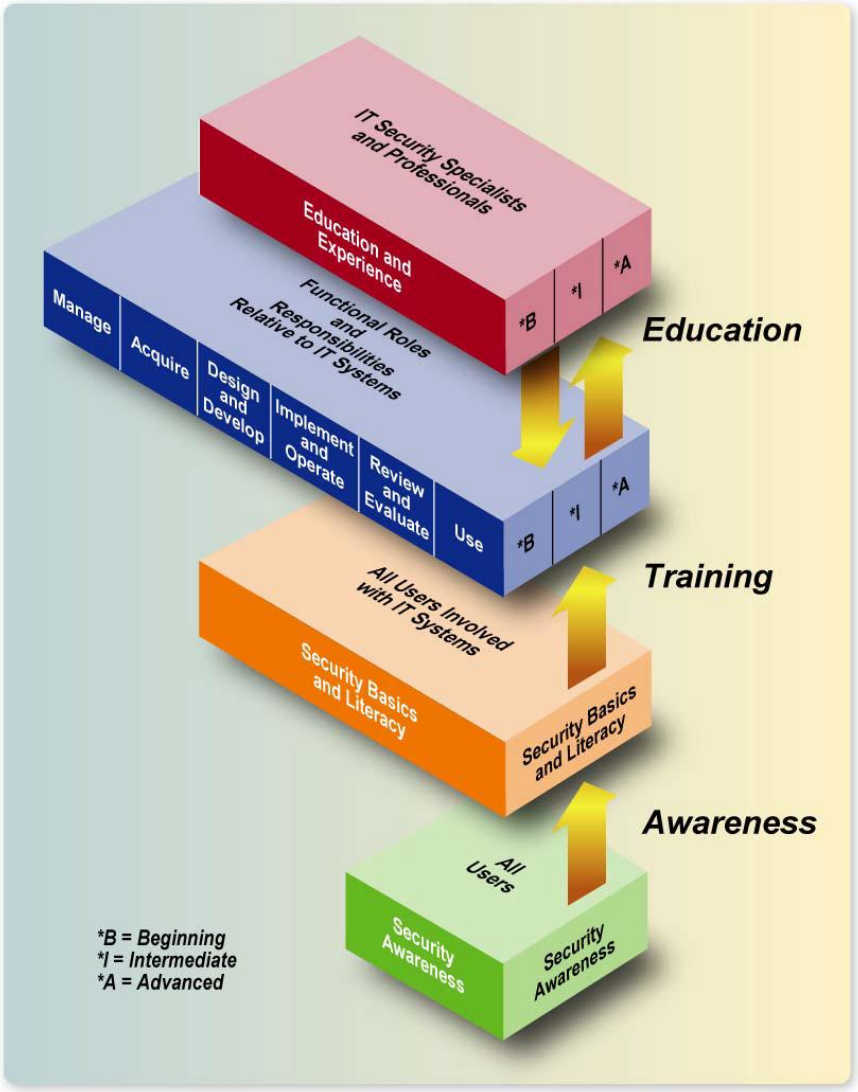
Telecommunication systems department

Lecturer: assistant professor Persikov Anatoliy Valentinovich

AWARENESS AND TRAINING

The **security awareness and training program** is a critical component of the information security program. It is the vehicle for disseminating security information that the workforce, including managers, need to do their jobs. In terms of the total security solution, the importance of the workforce in achieving information security goals and the importance of training as a countermeasure cannot be overstated. Establishing and maintaining a robust and relevant information security awareness and training program as part of the overall information security program is the primary conduit for providing the workforce with the information and tools needed to protect an agency's vital information resources. These programs will ensure that personnel at all levels of the organization understand their information security responsibilities to properly use and protect the information and resources entrusted to them. Agencies that continually train their workforce in organizational security policy and role-based security responsibilities will have a higher rate of success in protecting information.

AWARENESS AND TRAINING



AWARENESS AND TRAINING POLICY

All users have information security responsibilities.

FISMA mandates that all users complete “awareness training,” though NIST publications call this “awareness.” FISMA also tasks agencies with identifying and training those individuals who have significant responsibilities for information security, a requirement formalized by OPM’s information security awareness and training policy promulgated in June 2004. OPM’s policy strengthens the FISMA requirement for user exposure to “awareness training” by adding “at least annually,” and requires agencies to provide “role-specific training” in accordance with NIST guidance. Although there is no federal mandate for formal education (provided by colleges or universities) and certification of information security professionals, they are mentioned in this section since some agencies include them as part of a comprehensive training solution for federal employees.

COMPONENTS: AWARENESS, TRAINING, EDUCATION, AND CERTIFICATION

An agency's information security program policy should contain a clear and distinct section devoted to agency-wide requirements for the awareness and training program. Although security awareness and training is generally referred to as "a" program, many organizations consider awareness and training to be two distinct functions, each with separate purposes, goals, and approaches.

Proper implementation of these components (with consideration of options like education and professional certification) promotes professional development, which leads to a high-performance workforce.

Requirements for the security awareness and training program should be documented in the 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.

AWARENESS

Security awareness is a blended solution of activities that promote security, establish accountability, and inform the workforce of security news. Awareness seeks to focus an individual's attention on an issue or a set of issues. Awareness is a program that continually pushes the security message to users in a variety of formats.

An awareness program includes a variety of tools, communication, outreach, and metrics development.

- **Tools**. Awareness tools are used to promote information security and inform users of threats and vulnerabilities that impact their agency and "personal" work environment by explaining the "what" but not the "how" of security, and communicating what is and what is not allowed. Awareness is used to explain the rules of behavior for using an agency's information systems and information and establishes a level of expectation on the acceptable use of the information and information systems. Types of tools include:
  - Events, such as a security awareness day;
  - Promotional materials;
  - Briefings (program- or system-specific- or issue-specific); and
  - Rules of behavior.

AWARENESS

- **Communication.** A large part of an awareness effort is communication with users, managers, executives, system owners, and others. A communications plan is needed to identify stakeholders, types of information that is to be disseminated, channels for disseminating information, and the frequency of information exchanges. The plan also identifies whether the communications are one-way or two-way. Activities that support communication include:
  - Assessment (as is/to be models);
  - Strategic plan; and
  - Program implementation.
- **Outreach**. Outreach is critical for leveraging best practices within the federal sector. It has two elements for intra- and interagency awareness. The intra-agency element promotes internal awareness of information security. A Web portal that provides a one-stop-shop for security information can be an effective outreach tool. Policy, frequently asked questions (FAQs), security e-newsletters, links to resources, and other useful information are easily accessible to all employees. This tool promotes a consistent and standard message. The interagency element promotes sharing among agencies and is used to leverage awareness and training resources.

TRAINING

Information security training strives to produce relevant and needed security knowledge and skills within the workforce. Training supports competency development and helps personnel understand and learn how to perform their security role. The most important 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 a set of issues.

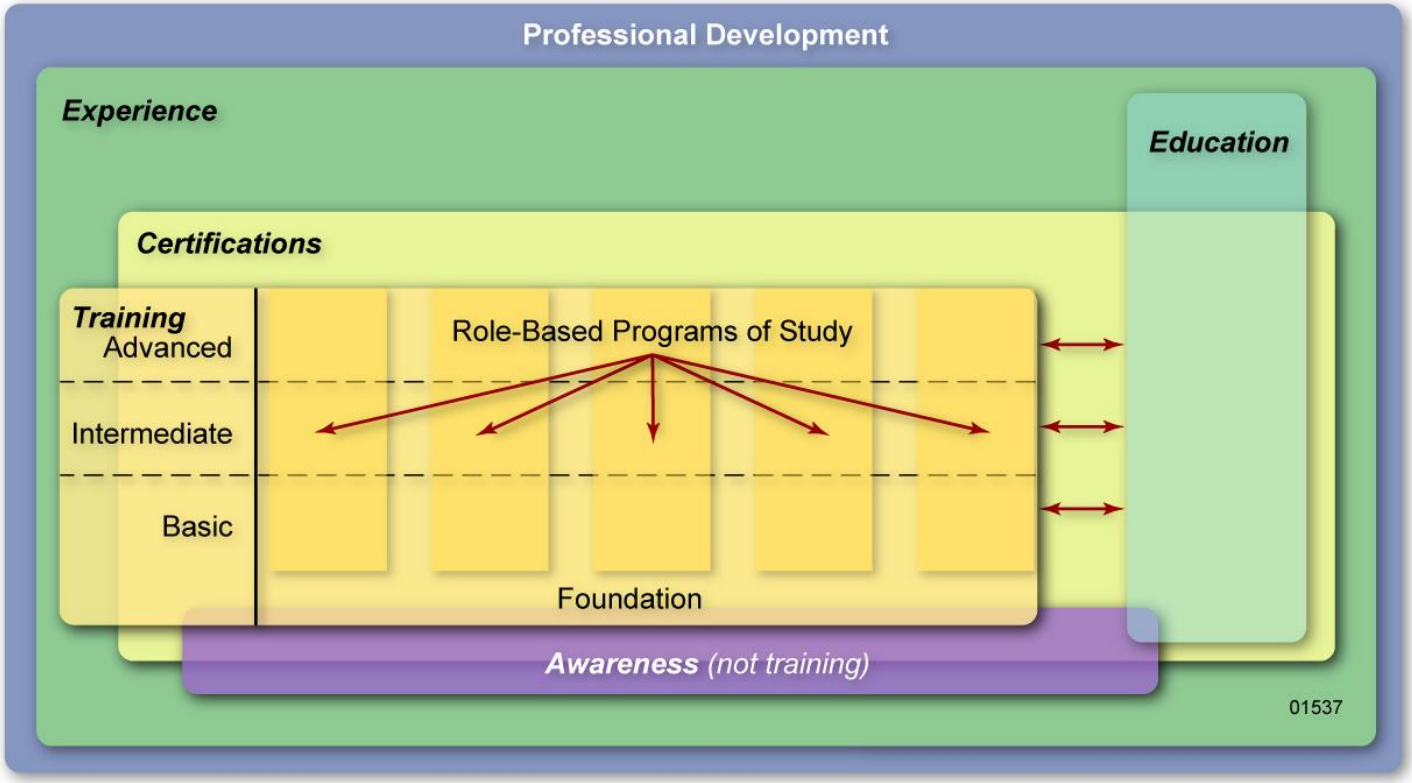
Role-based training provides security courses that are tailored to the specific needs of each group of people who have been identified as having significant responsibilities for information security in their organization. NIST SP 800-16 provides guidance for establishing role- and performance-based security training programs.

EDUCATION

Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and adds a multidisciplinary study of concepts, issues, and principles (technological and social). Information security education strives to produce information security specialists and professionals who are capable of vision and proactive response. Several colleges and universities provide academic programs to support the information security needs of the public and private sectors. Many of these schools partner with the federal sector to accomplish research and development tasks to improve information security.

CERTIFICATION

In response to the growing demand for information security personnel within federal agencies, there has been a movement toward increased professional standards for federal and contracted security personnel. This "professionalization" integrates training, education, and experience with an assessment mechanism to validate knowledge and skills, resulting in the "certification" of a predefined level of competence.



CERTIFICATION

It should be noted that there are distinct differences among certifications that are offered by a variety of organizations. Primarily, one will encounter certificates of completion, certifications awarded by an industry and/or vendors, and graduate-level certificates awarded by academic institutions:

- Certificates of completion are provided to individuals solely as a testament to completion of a particular course – these certificates do not make any claims that the individual actually gained knowledge and/or skills.
- Industry and/or vendor certification requires a combination of training, education, and experience. These certifications validate knowledge and skills through testing – they provide varying degrees of assurance that an individual has a baseline level of knowledge, skills, and abilities (KSAs) with regard to a predefined body of knowledge. The preparatory work for knowledge-based or skill-based certifications normally includes training in a prescribed body of knowledge or technical curriculum.
- Graduate certificates in information security are awarded by an academic institution to individuals who successfully complete all graduation requirements for a particular program. These graduate certificates generally require 18 to 21 credit hours of academic study, have at least four required courses, allow for one or two electives, and may require some form of research paper, project, or case study.

DESIGNING, DEVELOPING, AND IMPLEMENTING AN AWARENESS AND TRAINING PROGRAM

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

1) Designing the program (including the development of the information security awareness and training program plan);
2) Developing the awareness and training material; and
3) Implementing the program.

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

DESIGNING AN AWARENESS AND TRAINING PROGRAM

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

Designing an information 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 agency-wide awareness and training plan is developed, organizational buy-in is sought and secured, and priorities are established.

DEVELOPING AN AWARENESS AND TRAINING PROGRAM

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).
- "What skill or skills do we want the audience to learn and apply?" (training and education).

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 so impersonal and general that it could be given 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, current, and relevant.

DEVELOPING AN AWARENESS AND TRAINING PROGRAM

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 information 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 AWARENESS AND TRAINING PROGRAM

An information 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 information 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. Since there are several ways to present and disseminate awareness and training material throughout an organization, agencies should tailor their implementation to the size, organization, and complexity of their enterprise.

POST-IMPLEMENTATION

An organization's information security awareness and training program can quickly become obsolete if sufficient attention is not paid to technology advancements, IT infrastructure changes, organizational changes, and shifts in organizational mission and priorities.

CIOs and senior agency information security officers (SAISOs) need to be cognizant of this potential problem and incorporate mechanisms into their strategy to ensure that 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." Efforts supporting this post-implementation feedback loop should be developed in consideration of the security organization's overall ongoing performance measures program.

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 on program activity (e.g., courses, dates, audience, costs, sources). The tracking system should capture this data at an agency level, so it can be used to provide enterprise-wide 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 follow-up 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 and training 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), 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.

MANAGING CHANGE

It is necessary to ensure that the program, as structured, continues to evolve 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 on how best to design training solutions and content. Emerging issues, such as homeland defense, will also impact the nature and extent of security awareness and training activities necessary to keep users informed and/or trained about the latest threats, vulnerabilities, 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 policies evolve, awareness and training material should reflect these changes.

PROGRAM SUCCESS INDICATORS

CIOs, program officials, and SAISOs should be primary advocates for awareness, training, education, and professionalization. Securing an organization's information and infrastructure is a team effort, requiring the dedication of capable individuals to carry out their assigned security roles within the organization. Listed below are some key indicators to gauge the support for, and acceptance of, the program:

- Key stakeholder demonstrates commitment and support;
- 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;

PROGRAM SUCCESS INDICATORS

- 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.

THANKS FOR ATTENTION