Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Developing an Integrated Security Training, Awareness, and Education Program

This essay will illustrate how to successfully implement a comprehensive Security Training, Awareness, and Education program federal arena, however these processes are applicable and utilized in commercial organizations as well by using the Instructional System Design (ISD) process or model. This will prove that "ISD is an effective model for the creation and revision of instruction", (Lopez, Wollert). The ISD model is not only flexible and engaging, but it "ensures total quality in the education and training environme...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

Developing an Integrated Security Training, Awareness, and Education Program

By

Courtney Gilbert

June 2003

GSEC Practical Assignment version 1.4b

Option 1

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

Since the terrorist attacks on the United States on September 11, 2001, corporations and government organizations alike have brought Security Training, Awareness, and Education into the spotlight. Once thought of as "just filling a mandatory requirement" or "I have to do this because my boss told me too," is not the perception now. There was a time when organizations were going through some tough times and trainers would be the first to let go. These are very different times indeed.

This essay will illustrate how to successfully implement a comprehensive Security Training, Awareness, and Education program federal arena, however these processes are applicable and utilized in commercial organizations as well by using the Instructional System Design (ISD) process or model**.** This will prove that "ISD is an effective model for the creation and revision of instruction", (Lopez, Wollert). The ISD model is not only flexible and engaging, but it "ensures total quality in the education and training environment by continuously evaluating the process and products", (AFMAN). I will define and describe how the ISD process coupled with National Institute of Standards and Technology Special Publication (NIST SP) 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model,* can be used to effectively carry out this mission.

Objective

An Integrated Security Training, Awareness, and Education Program must be based on a validated training strategy and include a formal course curriculum in addition to other learning interventions designed to deliver the appropriate security information and messages to all levels of employees. To do this, a broad program that includes training, education, awareness, and outreach must be developed to deliver a multitude of security messages through various means to all employees. Formal, instructor led training, computer or Internet-based training, videos, conferences, forums, and other technology based and traditional delivery methods are all examples of what must be part of the Integrated Security Training, Education, and Awareness Program.

Integrated Security Training, Awareness, and Education Technical Approach

To successfully apply and integrate proven courseware design methodologies and an integrated security training model against the myriad and diverse subjects that compose integrated security training, awareness and education. Process-driven methodologies are a must. Proven methodologies such as the Instructional Systems Design (ISD) process and the National Institute of Standards and Technology Special Publication (NIST SP) 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

represent proven best practices in security training. It is important to address both training and security issues.

The information that follows describes the approach to integrated security training, awareness and education and how to perform the following tasks.

- Apply Instructional Systems Design (ISD) processes to security topics
- Apply NIST SP 800-16 to provide the right content for the right people
  - Identify target audience for security training
  - Map out the core body of knowledge to identify the appropriate level of training
- Design and develop security awareness and training programs to support role- and performance-based security needs
- Technical training
- Management training
- Security awareness
- Outreach
- Deliver knowledge- and skill-based training by personnel that are both qualified security professionals and experienced trainers

Although I present the ISD processes and NIST SP 800-16 model separately in this essay to promote understanding and to minimize confusion, I apply them simultaneously when approaching the Integrated Security Training, Awareness, and Education tasks.

Apply ISD Process

To ensure that you meet the organizations needs in a valid, reliable, and cost-effective manner, apply the ISD process to all security training, education, and awareness tasks. The process is the result of proven experience in instructional research and development of academic, federal, military and commercial organizations. “Meeting the business objectives of the organization and understanding the customers’ needs are what the goal of a security program is about”, (Krause, Tipton p.198). Standardized methodologies such as ISD are critical to successful training programs. It ensures a "best practices" approach to training development and emphasizes quality in the resulting products. The ISD process consists of five basic steps or phases: analysis, design, development, implementation and evaluation.

Step 1—Analysis

The first phase of the ISD process consists of the collection and analysis of data. The methods of analysis include individual interview, focus group, observation, and study of courseware, work samples, reports and records. The result of the analysis step is a clear definition of *who* needs to be trained in *what* content areas and *why*. Walter Dick and Lou Carey define this as, “the formal process of

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

identifying discrepancies between current outcomes and desired outcomes for an organization," (Carey, Dick). The analysis phase focuses on an analysis of each of the following items:

- Audience—identification of the individuals or groups that require integrated security training, education, and awareness
- Needs—identification of the security learning needs for the client's workforce.
- Tasks—identification of processes, tools, conditions, and requirements for accomplishment of integrated security tasks that are appropriate for the target audience.

Understanding that some organization needs can best be addressed via distance learning, web-based, CD ROM, or other e-learning solutions prove to be a cost-effective training tool. This approach can consistently and simultaneously be an effective delivery method to large organizations and geographically dispersed sites. You must keep in mind that the delivery environment must be stable. To this end, the delivery environment must be accurately identified and evaluated to determine minimum configurations and parameters for conducting training via these methods. With this in mind, a technology assessment is conducted early in the process to assess the delivery environment, to determine what technologies are required to support an e-learning service offering and student load, and to identify the level of service that is required.

Additional security concerns must be addressed if the e-learning is to be delivered in a sensitive or classified environment. For example, web-based or web-enabled solutions may use Java, Cold Fusion, or MacroMedia's Flash technologies. Use of these or other technologies must be approved for the delivery environment. If there are security issues for using e-learning hardware and/or software, it is important to coordinate with appropriate security officers or appropriate management to ensure that implementation of training solutions does not compromise the integrity or security of the system.

Step 2—Design

Once the variables have been identified and clarified, design of the curriculum can begin. In this phase, the tasks include:

- defining performance objectives,
- identifying evaluation methods,
- identifying delivery methods, and
- creating an outline of the information flow and organization, material and activities.

The first task in the course design process is to develop performance objectives and one or more criterion that measures learners' success in attaining the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

objective. Specific behaviors called out in the objectives and criteria guide the selection of appropriate delivery methods and media. There are three types of behavioral objectives that reflect the level of learning involved: knowledge, skill and ability. The performance objectives are phrased so that the end result of the learning is measurable. These objectives naturally lead into a methodology for evaluating student learning. In the next task, evaluation criteria are developed based on the objectives of the learning program. Donald Kirkpatrick's model includes four levels of evaluation. They are:

- Level 1 - reaction,
- Level 2 - learning,
- Level 3 – transfer
- Level 4 – results (Winfrey)

During this step of the process, it is time to create an evaluation plan. Writing the plan at this point helps to ensure that evaluation is built into the development of the instructional material. It also helps to ensure the integration of the evaluation phase into each of the remaining steps of the ISD process. This plan focuses on:

- what needs to be evaluated
- what data resources are required to meet the evaluation needs
- how the data should be analyzed
- how the results should be reported

It is important to identify and create evaluation methods that support the organizations mission. Based on the needs of the target audience, you then can anticipate what level evaluation is necessary. It is possible that a combination of evaluation levels can be used simultaneously.

Given the need, task, and audience, the appropriate method of delivery is identified. The medium could include instructor-led training, self-study, job aids, and computer-based training (web, CD-ROM, or a combination). In selecting an appropriate instructional method, consider many factors:

- learning objectives (conceptual vs. procedural)
- performance requirements
- frequency of change or update to content
- learning style of audience
- available resources
- practical limitations

The final task of this step is to create a course outline/design document that will serve as a reference for the remaining steps of the process. For each course segment, it specifies:

- objectives

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- topics to be covered
- level of learning (knowledge, skill or competence)
- instructional method and media
- learning activities and exercises
- evaluation criteria

Step 3—Develop

The instructional materials are created and refined in the development phase. The phase follows a general three-pronged process of draft, review, and revision. Since instructor-led training is usually an option for course delivery, this phase will also include:

- creating materials for the training of trainers (if required)
- creating materials for the training of students
- developing hands-on activities for usability testing

At this stage of the process, it is necessary to develop the training materials, validate the materials with individual and group testing, and deliver the validated training packages to the target audience.

Step 4—Implement

Implementation or delivery is the fourth step in the ISD process. This step is perhaps the most familiar to trainers (Benkowski, Rothwell, p.141). The implementation phase includes the steps necessary to execute the instruction. A number of important steps highlight this phase:

- preparing a master training plan to guide implementation activities
- preparing the required facilities (location, equipment, and materials)
- conducting pilot programs with the target audience

Implementation begins before production of final materials is actually complete. Pilot presentations to students representative of the target population occur before the materials are finalized. During this phase, courseware and documentation changes are made as needed.

Step 5—Evaluation and Maintenance

The evaluation phase encompasses the procedures and techniques for measuring and maintaining instructional quality control standards. Ensure that there is a positive transfer of knowledge and skills from the training environment to the job. The primary focus of evaluation is student mastery and instructional presentation. The main issues to address in evaluation include:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Does the training affect the desired change in students' performance?
- Does the training enable students to achieve the objectives?
- Does the training meet the client's needs?

Apply NIST SP 800-16—IT Security Instructional Model

The IT Security Learning Continuum from NIST SP 800-16, shown in Exhibit 1, represents the instructional best practice for IT Security Awareness, Training, and Education Programs. The model is created from requirements of several Federal regulations to include OMB Circular A-130, Appendix III.

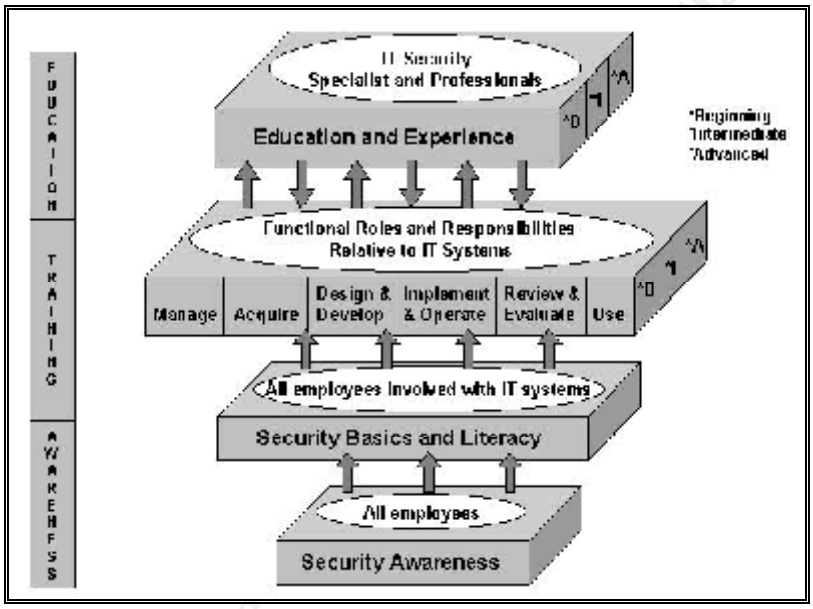

Exhibit 1: Information Technology Security Learning Continuum (NIST p.13)

Awareness, in this context, refers to a learning process that changes individual and organizational attitudes and perceptions to realize the importance of security and the adverse consequences of its failure. Awareness is not training, but rather a presentation or briefing. Awareness relies on reaching a broad audience through marketing and attractive packaging techniques. The awareness-level of instruction precedes training, which is more formal. ***Training*** builds knowledge and skills to augment and enhance job performance and enables people to perform more effectively. ***Education*** is an advanced form of training. It leverages experience in a field of study to further enhance and develop knowledge, skills and abilities. Exhibit 2 presents Dorthea deZafra's "Comparative Framework" for instructional levels that illustrates the instructional differences among awareness, training, and education.

COMPARISON ELEMENTS	AWARENESS	TRAINING	EDUCATION

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Learning Objective:	Recognition and Retention	Skill	Understanding
Example Teaching Method:	Media – Videos – Newsletters – Posters	Practical Instruction – Lecture/demo – Case study – Hands-on practice	Practical Instruction – Seminar/discussion – Reading and study – Research
Test Measure:	True/False Multiple Choice (identify learning)	Problem Solving i.e., Recognition and Resolution (apply learning)	Essay (interpret learning)
Impact Timeframe:	Short-term	Intermediate	Long-term

Exhibit 2: Comparative Framework

The model defines three distinct levels of IT security training: beginning, intermediate, and advanced. Training at the ***beginning*** level specifically targets the *novice*. It provides "foundation" training to support performance of a specific security role. Training at the ***intermediate*** level targets the *journeyman* with training to enhance his/her breadth and/or depth of security knowledge and skill. It is used to cultivate both security generalists and specialists. Training at the ***advanced*** level offers IT security technicians and professionals the opportunity to apply knowledge and skill attained through training to mission critical IT security problem solving and technology assessment.

Identify Target Audience

The model provides flexibility to define the right training for the right people. The table in Exhibit 3 identifies the job categories that compose the technical and non-technical target audiences. A primary objective for cyber security training is to "bridge the gaps" that exist between security and technology professionals. Historically, these professionals coexisted as parallel lines - each operated in its own domain and neither understood the other very well. Today, there is a convergence of the two domains—each recognizes the other and is beginning to have an understanding and appreciation for their interdependencies. As we move to the future, the lines will merge and move forward together as a single entity. As this transition occurs, it becomes critical that the right people get the right security training. It is also of paramount importance that the non-technical workforce understands their role in protecting information and information resources.

TECHNICAL AUDIENCE	NON-TECHNICAL AUDIENCE

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Security Professionals • Information System Security Officer (ISSO) • Information System Security Manager (ISSM) • Security Engineers **Administrators** • Network • System • Database • E-mail/v-mail **Programmers** • System • Application	**Managers** • Executives/Officials • Managers of technical staff • Managers of non-technical staff **System Owners** • Networks (WANs/LANs) • Application systems • Database **Other Personnel** • Legal Affairs • Contracting Officers • Human Resources • General users

Exhibit 3: Target Audience Categories

Insiders pose the largest threat to any IT system and that those insiders with the greatest access and privileges are the greatest threat. Training is an effective means to counter this threat and mitigate the associated risks.

Identify Core Body of Knowledge

To keep pace with technology, the body of knowledge associated with IT security is vast and growing at an accelerated rate. Regardless of its size and growth rate, there are fundamental IT security concepts that establish a foundation for training and education. These fundamental concepts, defined in NIST SP 800-16 and National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4011, *National Training Standard for Information Systems Security (INFOSEC) Professionals,* compose the core body of knowledge (CBK) that is prerequisite to role- and performance-based security training. The CBK is comprised of the following topics:

- Laws and regulations
- IT security program
- System environment
- System interconnection
- Information sharing
- Risk Management
- Life Cycle controls
- Management controls
- Operational controls
- Technical controls
- Awareness, training, and education
- Handling sensitive and classified information

These topics are the building blocks that establish the foundation for a successful and relevant Integrated Security Training, Awareness, and Education program.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Design and Develop Security Awareness and Training Programs

This section addresses the specific security training needs of an organization and presents a training approach for satisfying those needs. User awareness the linchpin to achieving security goals. It is the cornerstone to security training for the non-technical component of the workforce. IT security is a "people issue" and awareness programs address common "people" problems. Employees want to do what is right, but they frequently don't know what that is. We know that solutions for yesterday's security issues are obsolete today, and the security solutions we have today may be obsolete tomorrow. The security environment is constantly changing and the variety of solutions is growing at a phenomenal rate. Awareness is a crucial element in addressing these issues. Informative and engaging awareness programs are a viable and effective means of informing the workforce of changes in security policies, procedures and practices.

TYPE OF TRAINING	TARGET AUDIENCE	KNOWLEDGE AND SKILLS
Technical	Security Professionals Administrators Programmers	• Core Body of Knowledge • Operating Systems • Applications • Protocols • Security tools • Technical controls • Policy and procedures • Risk Assessment • Security Plans • Certification and accreditation
Management	Executives/Officials Managers of technical staff Mangers of non-technical staff Systems Owners Contracting Officers Legal Affairs Human Resources	• Core Body of Knowledge • Risk Management • Security controls within system life cycle • Resource requirements • Contracting requirements • Policy and procedures
Security Awareness	All personnel	• Roles and responsibilities • Policy and procedures

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Exhibit 4: Potential Programs of Instruction

Exhibit 4 enumerates the types of training and the IT security knowledge and skills that would benefit the target audience categories identified in Exhibit 3. From this mapping of target audience to knowledge and skills, a training program can be developed to accommodate students at beginning, intermediate, and advanced levels of knowledge. Security training is identified to satisfy role- and performance-based needs of the organization and to provide both knowledge- and skill-based courses to enhance the security posture of the workforce. A focused and flexible security program can be tailored and published in a security training guide that identifies existing courses that satisfy level of knowledge and skill requirements. The immediate need is to identify courses to address the most critical and pressing deficiencies. A program such as this can be readily adapted in a dynamic security environment.

Conclusion

The importance of security training, awareness, and education is now more than ever a priority with private and public entities alike. The ISD process or model proves itself to be an invaluable methodology. ISD's step-by-step process lays out the groundwork for an effective program that is flexible and is adaptable to revisions at various points in the process. Perhaps, the most beneficial aspect of ISD is that it is a continuous cycle that allows revision to assess against quantitative and qualitative values to see if the problem that is trying to be solved is actually getting corrected.

Bibliography

"National Training Standards for Information Security (INFOSEC) Professionals." NSTISSI No.41. 20 June 1994. http://www.nstissc.gov/Assets/pdf/4011.pdf (19 June 2003)

"Information Technology Security Training Requirements: A Role- and Performance-Based Model." NIST Special Publication 800-16. April 1998

Winfrey, Elaine C. "Kirkpatrick's Four Levels of Evaluation." http://coe.sdsu.edu/eet/Articles/k4levels/index.htm (19 June 2003)

Benkowski, Joseph A. Rothwell, William J. "Building Effective Technical Training." San Francisco: Jossey-Bass/Pfeiffer, 2002. p. 124-142

Krause, Micki. Tipton, Harold F. "Information Security Handbook" 4th edition. Boca Raton: Auerbach, 2000. p. 197-212

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Carey,L. Dick,W. “Systems Approach Model for Designing Instruction.” http://162.105.142.5/instruction-design/materials2/Dick%20&%20Carey.htm (19 June 2003)

Lopez, T. Wollert, T. “Systems Approach to Training.” http://www.fletc.gov/red/powerpoint/Isd3_files/v3_document.htm (19 June 2003)

AFMAN 36-2234. 1 November 1993. http://www.au.af.mil/au/awc/awcgate/edref/36-2234-ISDnew.pdf (19 June 2003)

© SANS Institute 2003, Author retains full rights.

Last Updated: August 28th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

FOR578 Cyber Threat Intelligence	**Tysons Corner, VAUS**	**Aug 31, 2015 - Sep 04, 2015**	**Live Event**
SANS Milan 2015	**Milan, IT**	**Sep 07, 2015 - Sep 12, 2015**	**Live Event**
SANS Crystal City 2015	**Crystal City, VAUS**	**Sep 08, 2015 - Sep 13, 2015**	**Live Event**
SANS Network Security 2015	**Las Vegas, NVUS**	**Sep 12, 2015 - Sep 21, 2015**	**Live Event**
SANS Seoul 2015	**Seoul, KR**	**Sep 14, 2015 - Sep 19, 2015**	**Live Event**
SANS Tallinn 2015	**Tallinn, EE**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS Perth 2015	**Perth, AU**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS Baltimore 2015	**Baltimore, MDUS**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
Data Breach Investigation Summit & Training	**Dallas, TXUS**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS ICS Amsterdam 2015	**Amsterdam, NL**	**Sep 22, 2015 - Sep 28, 2015**	**Live Event**
SANS Bangalore 2015	**Bangalore, IN**	**Sep 28, 2015 - Oct 17, 2015**	**Live Event**
SANS DFIR Prague 2015	**Prague, CZ**	**Oct 05, 2015 - Oct 17, 2015**	**Live Event**
SANS Seattle 2015	**Seattle, WAUS**	**Oct 05, 2015 - Oct 10, 2015**	**Live Event**
SOS: SANS October Singapore 2015	**Singapore, SG**	**Oct 12, 2015 - Oct 24, 2015**	**Live Event**
SANS Tysons Corner 2015	**Tysons Corner, VAUS**	**Oct 12, 2015 - Oct 17, 2015**	**Live Event**
SANS Gulf Region 2015	**Dubai, AE**	**Oct 17, 2015 - Oct 29, 2015**	**Live Event**
SANS Cyber Defense San Diego 2015	**San Diego, CAUS**	**Oct 19, 2015 - Oct 24, 2015**	**Live Event**
SANS Tokyo Autumn 2015	**Tokyo, JP**	**Oct 19, 2015 - Oct 31, 2015**	**Live Event**
SANS South Florida 2015	**Fort Lauderdale, FLUS**	**Nov 09, 2015 - Nov 14, 2015**	**Live Event**
SANS Sydney 2015	**Sydney, AU**	**Nov 09, 2015 - Nov 21, 2015**	**Live Event**
SANS London 2015	**London, GB**	**Nov 14, 2015 - Nov 23, 2015**	**Live Event**
Pen Test Hackfest Summit & Training	**Alexandria, VAUS**	**Nov 16, 2015 - Nov 23, 2015**	**Live Event**
SANS Hyderabad 2015	**Hyderabad, IN**	**Nov 24, 2015 - Dec 04, 2015**	**Live Event**
SANS Chicago 2015	**OnlineILUS**	**Aug 30, 2015 - Sep 04, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**