InfoSec Services Hawaii (ISSH)
A Division of Computer-Aided Technologies International, Inc. (CATI)

Course Catalog
September 2000

InfoSec Services Hawaii
A Division of
Computer-Aided Technologies International, Inc.

Developing an InfoSec Awareness, Education, and Training (AET) Program – First Steps

Learning Objectives

This half-day workshop-style course provides an overview of how to develop and implement an AET Program. Participants will gain a broad perspective on developing and implementing AET Programs that make good business sense.

Workshop Focus and Features

Management's business concerns and employee attitudes are critical elements in protecting the information assets of an organization. In this course, learn how to develop and implement a comprehensive Information Security Awareness, Education, and Training Program that will keep everyone, from senior management to employees and staff, informed and motivated to pay attention to information protection, based on business needs. Receive practical ideas in this train-the-trainer course.

Prerequisites for this Course

None. No advance preparation required.

Program Level

Basic – covers fundamental principles and skills

Who Should Attend

MIS Directors/Managers
VP Information Systems
Information Security Managers
Information Security Consultants
Information Security Trainers
Systems Analysts
Systems Administrators
Senior Analysts
LAN Administrators
Network Administrators
Technologists

Human Resource Managers
Human Resource Staff
Educators

Program Content

Designing, Developing, and Implementing an AET Program

- Mind-Map (Brainstorming ideas to kick it off) **Group Exercise**
- Why an InfoSec Web Site is needed
- Contact Information - Customer Service Issues
- Publicity/Advertising
- Training Delivery Methods
- Types of Courses
- Sources of InfoSec Information

Tools of the Trade – Videos

- Why a comprehensive Information Security AET Program uses Awareness Videos
- Creating a video-lending library
- Awareness Video Vendors
- Awareness Video Activities
- Earmarking Funds to Buy Awareness Videos
- The viewing of selected Awareness Videos

Advance Preparation Required

None.

Instructional Method

Lecture-based, hands-on workshop style.

Fields of Study

Management

Recommended Continuing Professional Education (CPE) Credit

3 CPE

Communicating and Disseminating InfoSec Information Across the Business or Educational Enterprise

Learning Objectives

This half-day workshop-style course provides participants with an overview of how to create an in-house InfoSec program, which includes dissemination and communication of InfoSec information.

Workshop Focus and Features

Management's business concerns and employee attitudes are critical elements in protecting the information assets of an organization. In this course you will learn how use an Intranet to communicate and disseminate Information Security Awareness, Education, and Training (AET) information. Participants will also learn to develop awareness materials and to create awareness activities. This course will provide participants with the knowledge of how to communicate and disseminate information to everyone from senior management to employees and staff. Many methods of communication can be used to keep the users informed and motivated to pay attention to information protection for the sake of the business needs. Receive practical ideas in this train-the-trainer course.

Prerequisites for this Course

None. No advance preparation required. At the conclusion of this workshop, participants will be able to provide content to someone on their team at work to implement a Web-Site. The scope of this course does not cover how to code in HTML. The focus of this course will be on how to use an Intranet as a vehicle to communicate and disseminate information, as well as other methods for communicating Information Security Awareness.

Program Level

Basic – covers fundamental principles and skills.

Who Should Attend

MIS Directors/Managers
VP Information Systems
Information Security Managers
Information Security Consultants
Information Security Trainers
Systems Analysts
Systems Administrators

Senior Analysts
LAN Administrators
Network Administrators
Technologists
Human Resource Managers
Human Resource Staff
Educators
Web Developers

Program Content

Using an Intranet to Communicate and Disseminate AET Information

Recommended Intranet Structure

- Contact Information
- Awareness Activities
- InfoSec Course Information
- Policy Documents
- Sources of InfoSec Information
- Frequently Asked Questions (FAQ)

Tools of the Trade – Giveaways and Awareness Activities

- Recommend developing a unique mascot for your Awareness, Education, and Training Program
- Humor, Candy, Props
- Giveways
- Awareness Activities

Group Exercise

Advance Preparation Required

None.

Instructional Method

Lecture-based, hands-on workshop style.

Fields of Study

Management

Recommended Continuing Professional Education (CPE) Credit

3 CPE

Instructor-Led Training and Winning Presentation Techniques

Learning Objectives

This half-day workshop-style course provides an overview of how to conduct Instructor-Led Training Courses and how to create winning presentations.

Workshop Focus and Features

Planning, preparing, practice, and delivery equal successful presentation and facilitation sessions. Participants learn to create and deliver presentations that win audiences over to the importance of their message. Participants will learn how to deliver their message with impact. Receive practical ideas in this train-the-trainer course.

Prerequisites for this Course

None. No advance preparation required. However, participants will gain experience in giving presentations as part of this course. No advance work in preparing a presentation is required or expected.

Program Level

Basic – covers fundamental principles and skills.

Who Should Attend

MIS Directors/Managers
VP Information Systems
Information Security Managers
Information Security Consultants
Information Security Trainers
Systems Analysts
Systems Administrators
Senior Analysts
LAN Administrators
Network Administrators
Technologists
Human Resource Managers
Human Resource Staff
Educators

Program Content

Instructor-Led Training

- Objectives as Trainers
- How People Learn
- Using Humor
- Audience's Interest
- Trainer's Interest
- Neat ideas

Winning Presentation Techniques

- Instructional System Design
- Analyze Problem
- Design Lesson Plan
- Develop Your Approach
- Deliver Your Presentation
- Evaluation and Feedback

Group Exercise

Advance Preparation Required

None.

Instructional Method

Lecture-based, hands-on workshop style.

Fields of Study

Management

Recommended Continuing Professional Education (CPE) Credit

3 CPE

Developing Information Protection Publications and Policies, Plans, and Procedures

Learning Objectives

This half-day workshop-style course provides an overview on developing a variety of awareness publications, as well as experiencing steps for developing policies, plans, and procedures. Such publications promote good business practice and create industry-wide awareness with compliance for information protection.

Workshop Focus and Features

Participants will learn to create useful Information Protection publications and how to develop real-world InfoSec policies that make good business sense. Receive practical experience in hands-on exercises in this course.

Prerequisites for this Course

None. No advance preparation required.

Program Level

Basic – covers fundamental principles and skills.

Who Should Attend

Chief Technology Officers
Chief Information Officers
MIS Directors/Managers
VP Information Systems
Information Security Managers
Information Security Consultants
Information Security Trainers
Systems Analysts
Systems Administrators
Senior Analysts
LAN Administrators
Network Administrators
Technologists
Human Resource Managers
Human Resource Staff
Educators
Technical Writers

Program Content

Types of Publications Include

- Newsletters
- Bulletins/Alerts
- Announcements
- Tech Reports
- Cartoons
- Posters
- In-house Newspaper Articles
- Articles for Local/National Newspapers

Delivery Methods

- Hard-copy
- Electronic

Group Exercise

Overview of Developing and Implementing Policies, Plans and Procedures

Making it make sense

- Tie security goals to business objectives
- Information Protection Policy Statement
- Information Protection Mission Statement

Management Support

Development Project

- Goals, objectives, schedules, and deliverables

Information Protection Policy Table of Contents

Review Panel for Policies, Plans, and Procedures

Delivery Methods

Life-Cycle

Resources

Group Exercise

Advance Preparation Required

None.

Instructional Method

Lecture-based, hands-on workshop style.

Fields of Study

Management

Recommended Continuing Professional Education (CPE) Credit

3 CPE

Developing and Implementing a Comprehensive Awareness, Education, and Training (AET) Program for Information Management Officers (IMOs), Information System Security Officers (ISSOs), and Computer System Security Officers (CSSOs) in the U.S. Federal Government

Learning Objectives

This full-day workshop-style course provides an overview of how to develop and implement an AET. Participants will gain a broad perspective on developing and implementing AET Programs as required for IMOs, ISSOs, and CSSOs by the U.S. Department of Defense (DoD). These personnel are responsible for providing initial briefings, periodic training, and Security Awareness Programs.

Refer to background information below from:

- *National Computer Security Center - A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems*
- *Army Regulation AR 380-19*
- *U.S. Air Force Instruction AFI 33-202*
- *U.S. Air Force Instruction AFI 33-204*
- *U.S. Navy Department of the Navy Information Security Program (ISP) Regulation SECNAVINST 5510.30A (10 March 1999)*
- *U.S. Marines (compliance with SECNAVINST 5510.30A) – same as for the U.S. Navy.*

National Computer Security Center - A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems (May 1992)*, addresses Security Training in section 3.8*. This document specifies, “personnel are an integral part of the security protection surrounding an AIS that must understand the vulnerabilities, threats, and risks inherent with AIS usage. Therefore, computer security shall be included in briefings given to all new personnel. To reinforce this initial training and to introduce new concepts, periodic training and security awareness programs should be conducted. The ISSO shall continue training to keep current in security products and procedures. The ISSO is responsible for ensuring that:”

- “All personnel (including management) have computer security awareness training and have read applicable sections of the AIS security plan. This includes training in security procedures and use of security products. “
- “All users are educated regarding password management. “
- “Users understand the importance of monitoring their successful and unsuccessful logins, if possible. “

“The ISSO can keep users informed about security in many different ways. Some approaches follow: “

- “Periodically display messages on the AIS when the user logs onto the system. “
- “Develop and distribute security awareness posters to foster interest.“
- “Disseminate new security information about the system and issue reminder notices about protection procedures.“
- “Issues memos to notify users of changes.“
- “Provide “hands-on” demonstrations of AIS security features and procedures.“

Army Regulation 380-19, Chapter 2 Section VI Personnel Security, paragraph 2-15, addresses Training and awareness programs. This regulation specifies that “personnel who manage, design, develop, maintain, or operate Automated Information System (AIS) will undergo a training and awareness program. Such a program is to consist of an initial security training and awareness briefing. Such a briefing is to include information on threats, vulnerabilities, and risks associated with the information system, information security objectives (what needs to be protected?), responsibilities and accountability associated with system security, information accessibility, physical and environmental considerations, system data and access controls, emergency and disaster plans, authorized system configuration, and configuration management requirements. In addition to the initial security training and awareness briefing, periodic security training and awareness is required. Such periodic training and awareness may include various combinations of the following: self-paced or formal instruction, security education bulletins, security posters, training films and tapes, and computer-aided instruction. “

U.S. Air Force Instruction AFI 33-202 (1 February 1999)
Chapter 3- Minimum Requirements, Paragraph 3.14. Information Assurance Security Awareness, Training, and Education (SATE).

“All Air Force personnel will receive Information Assurance (IA) awareness, training, and education throughout their assignments according to AFI 33-204, *Information Protection Security Awareness, Training, and Education (SATE) Program.”*

U.S. Air Force Instruction AFI 33-204(26 April 1999) Information Protection Security Awareness, Training, and Education (SATE) Program.

“Section A – General Information, Paragraph 3. Objectives.”

“3.1. Understand the inherent weaknesses in information systems and the potential harm to national security due to the improper use of information systems. “

“3.2. Keep informed of the threats (including human intelligence) to, and vulnerabilities of, information systems. “

“3.3. Take necessary measures to protect information generated, stored, processed, transferred, or communicated by information systems. “

“3.4. Recognize practices and conditions that create vulnerabilities in information systems, and use established security procedures to address them. “

“3.5. Recognize the potential damage to national security if COMSEC material is compromised and understand the security measures required to protect this material. “

“3.6. Protect information systems against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of information systems or data. “

“3.7. Understand how COMPUSEC, COMSEC, and EMSEC relate to the overall protection of information generated, processed, stored, or transferred by information systems. “

Section B – Training.
Paragraph 4 General Requirements:

“All military and civilian personnel will receive four types of SATE training: accession, initial/recurring, awareness, and specialized. An individual trained in information protection principles and concepts will conduct this training. “

Paragraph 7. Awareness Training.

“The SATE program managers satisfy awareness training requirements by displaying information protection –related awareness aids, using public service announcements, or providing applicable articles form unit, base, and command publication to unit personnel. Managers will encourage the use of information protection screen savers and take advantage of local cable public service channels (Armed Forces Radio and Television Service overseas) to advance information protection awareness. “

U.S. Navy and U.S. Marines both must be compliant with SECNAVINST 5510.30A (10 March 1999)

Department of the Navy Information Security Program (ISP) Regulation SECNAVINST 5510.30A (10 March 1999)

Chapter 4 Security Education

Paragraph 4-1 Basic Policy states that:

“1. Each command handling classified information will establish an maintain an active security education program to instruct all personnel, regardless of their position, rank or grade, in security policies and procedures.”

“2. The purpose of the security education program is to ensure that all personnel understand the need and procedures for protecting classified information. The goal is to develop fundamental security habits as a natural element of each task.”

Paragraph 4-2 Responsibilities states that:

“1. Chief of Naval Operations Special Assistant for Naval Investigative Matters and Security (CNO (N09N)) is responsible for policy guidance, education requirements and support for the Department of the Navy (DON) security education program. Development of security education materials for use throughout the DON must be coordinated with CNO (N09N2) for consistency with current policies and procedures. This requirement does not apply to materials which are prepared for use in command programs.”

Paragraph 4-3 Scope states that:

“1. Security education must be provided to all personnel. The education effort must be tailored to meet the needs of the command, as well as those of different groups within the command.”

“2. In formulating a command security education program, the security manager must provide for the minimum briefing requirements of this regulation. Security managers must guard against allowing the program to become stagnant or simply comply with requirements without achieving real goals.”

Paragraph 4-1 Minimum Requirements states that:

“1. The following are the minimum requirements for security education:”

“a. Indoctrination of personnel upon employment by the DON in the basic principles of security.”

“b. Orientation of personnel who will have access to classified information at the time of assignment, regarding command security requirements.”

“c. On-the-job training in specific security requirements for the duties assigned.”

“d. Annual refresher briefings for personnel who have access to classified information.”

“e. Counterintelligence briefings once every 2 years for personnel who have access to information classified Secret or above.”

“f. Special briefings as circumstances dictate.”

“g. Debriefing upon termination of access.”

Paragraph 4-13 Training for Security Personnel

Sub Paragraph 4. states that:

“4. CNO (N09N2) publishes the “Information and Personnel Security Newsletter” on a quarterly basis. This newsletter is also posted to the CNO homepage. The newsletter is not a directive, but states interpretations of security policies and procedures and provides advance notification of changes to the program. A roster of personnel assigned to CNO (N09N2), showing each area of responsibility is published periodically and posted on the homepage to assist you in routing your telephonic requests.”

Paragraph 4-14 Security Awareness states:

“To enhance security, a security education program must include continuous and frequent exposure to current information and other awareness materials. Signs, posters, bulletin board notices, and Plan of the Day reminders are some of the media which should be used to promote security awareness.”

Workshop Focus and Features

This full-day train-the-trainer workshop will provide Information Management Officers (IMOs), Information System Security Officers (ISSOs), and Computer System Security Officers (CSSOs) with the knowledge to carry out their Awareness, Education, and Training Program responsibilities. The U.S. Federal Government's concerns and employee attitudes are critical elements in protecting National Security information and Sensitive But Unclassified information. In this course, IMOs, ISSOs, and CSSOs will receive a broad overview on how to develop and implement a comprehensive Information Security Awareness, Education, and Training Program that will keep all personnel informed, and motivated to pay attention to information protection. The course will include information for using an Intranet to communicate and disseminate InfoSec information. Participants will take part in hands-on exercises to develop Awareness Activities and/or Awareness Publications. Participants will receive practical ideas in this train-the-trainer course.

Prerequisites for this Course

An understanding of U.S. Federal Government requirements for IMOs, ISSOs, and CSSOs to provide Awareness, Education, and Training Programs.

Program Level

Basic to intermediate. Covers fundamental principles and skills, and builds on such skills in practical situations and extends them to a broader range of applications.

Who Should Attend

Information Management Officers (IMO)
Information System Security Officers (ISSO)
Computer System Security Officers (CSSO)

Program Content

Designing, Developing, and Implementing at AET Program

- Mind-Map (Brainstorming ideas to kick it off) **Group Exercise**
- Contact Information - Customer Service Issues
- Publicity/Advertising

- Types of Publications
    - Newsletters
    - Bulletins/Alerts
    - Announcements
    - Tech Reports
    - Cartoons
    - In-house newspaper articles
    - Articles from Local/National newspapers
- Delivery Methods
    - Hard-copy
    - Electronic
- Training Delivery Methods
    - Teaming for Training
    - Pros/Cons of Each Training Delivery Method
- Types of Courses
    - New Hire Orientation
    - Policy-Based Training
    - Awareness Courses
    - Application Specific (i.e., encryption software)
- Sources of Computer Security Information

Tools of the Trade – Videos

- Why a comprehensive InfoSec AET Program uses Awareness Videos
- Creating a video-lending library
- Awareness Video Vendors
- Awareness Video Activities
- The viewing of selected Awareness Videos
- Earmarking Funds to Buy Awareness Videos

Lunchtime includes a Group Exercise

Using an Intranet to Communicate and Disseminate AET Information

Recommended Intranet Structure

- Contact Information
- Awareness Activities
  - Awareness Video Information
  - Computer Security Day
- InfoSec Course Information
  - Description of Courses
  - Course Registration/Confirmation
  - Scheduled Courses
- Policy Documents
- Sources of InfoSec Information
- Frequently Asked Questions (FAQ)

Tools of the Trade – Giveaways and Awareness Activities

- Recommend developing a unique mascot for your Awareness, Education, and Training Program
- Humor, Candy, Props
- Giveways
- Awareness Activities

Group Exercise

Advance Preparation Required

None.

Instructional Method

Lecture-based, hands-on workshop style.

Fields of Study

Management

Recommended Continuing Professional Education (CPE) Credit

8 CPE

InfoSec Services Hawaii
Administrative Policies

Registration and Payment of Fees

Registration and confirmation for InfoSec Services Hawaii's training courses is conducted by e-mail via the Web-Site http://www.catii.com/infosecservices/. Registration is due and payable no later than 15 days prior to a course.

Cancellation

If it is necessary for you to cancel your registration, you are required to submit your cancellation in writing. We must receive your cancellation request no later than one week prior to the course. Payments are non-refundable. However, pre-paid fees may be transferred to a future course. In addition, *y*ou may, at any time, substitute another individual from your organization. Registrants who do not cancel and do not attend will be responsible for the full course fee. Please mail cancellations to: InfoSec Services Hawaii, 47-396 Kamehameha Highway, Kaneohe, Hawaii 96744-4736, or via e-mail to **infosec@catii.com**.

Questions may be sent by e-mail to **infosec@catii.com**, or please telephone (808) 521-2259.

If it is necessary for InfoSec Services Hawaii to cancel a course due to unforeseen circumstances, all registered participants will be notified by e-mail. The canceled course will be re-scheduled, and all participants will be given the opportunity to re-register. No refunds of payments will be issued. All pre-paid fees may be transferred to a future course, or you may substitute another individual from your organization.

Complaints

Send e-mail to **infosec@catii.com**. You may address complaints to Kenneth M. Goldstein, Executive Vice President, CATI.

Biography of Trainer

Gale S. Warshawsky is the Director of InfoSec Services Hawaii (ISSH), a Division of Computer-Aided Technologies International, Inc. (CATI). Her background includes extensive experience as a trainer. Ms. Warshawsky worked at Lawrence Livermore National Laboratory (LLNL) and at Visa International. She was responsible for the design, development, and implementation of their Information Security Awareness, Education, and Training Programs. She was honored by the Information Systems Security Association (ISSA) in 1994, with their Individual Achievement Award, and in 1995 as the Federal Information Systems Security Educators Association (FISSEA) Security Educator of the Year. Ms. Warshawsky has presented training workshops and seminars at many conferences to include: Department of Energy Computer Security Group Training Conferences, ISSA, Computer Security Institute (CSI), and MIS Training Institute.

NASBA
NATIONAL REGISTRY OF
CPE
SPONSORS

InfoSec Services Hawaii is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be addressed to the National Registry of CPE Sponsors, 150 Fourth Avenue North, Nashville, TN, 37219-2417. Telephone: 615-880-4200.