

CYBER LAW AND POLICY

Lesson 7 Security Program

Learning Objectives

- Describe the components of a security education, training, and awareness program and understand how organizations create and manage these programs

Components of the Security Program

- Information security needs of any organization are unique to the culture, size, and budget of that organization
- Determining what level the information security program operates on depends on the organization's strategic plan
 - In particular, on the plan's vision and mission statements
- The CIO and CISO should use these two documents to formulate the mission statement for the information security program

Information Security Roles

- Information security positions can be classified into one of three types: those that define, those that build, and those that administer
 - *Definers provide the policies, guidelines, and standards. They're the people who do the consulting and the risk assessment, who develop the product and technical architectures. These are senior people with a lot of broad knowledge, but often not a lot of depth.*
 - *Then you have the builders. They're the real techies, who create and install security solutions.*
 - *Finally, you have the people who operate and administrate the security tools, the security monitoring function, and the people who continuously improve the processes.*

Information Security Titles

- Typical organization has a number of individuals with information security responsibilities
- While the titles used may be different, most of the job functions fit into one of the following:
 - Chief Information Security Officer (CISO)
 - Security managers
 - Security administrators and analysts
 - Security technicians
 - Security staff

Figure 5-11

Information Security Roles

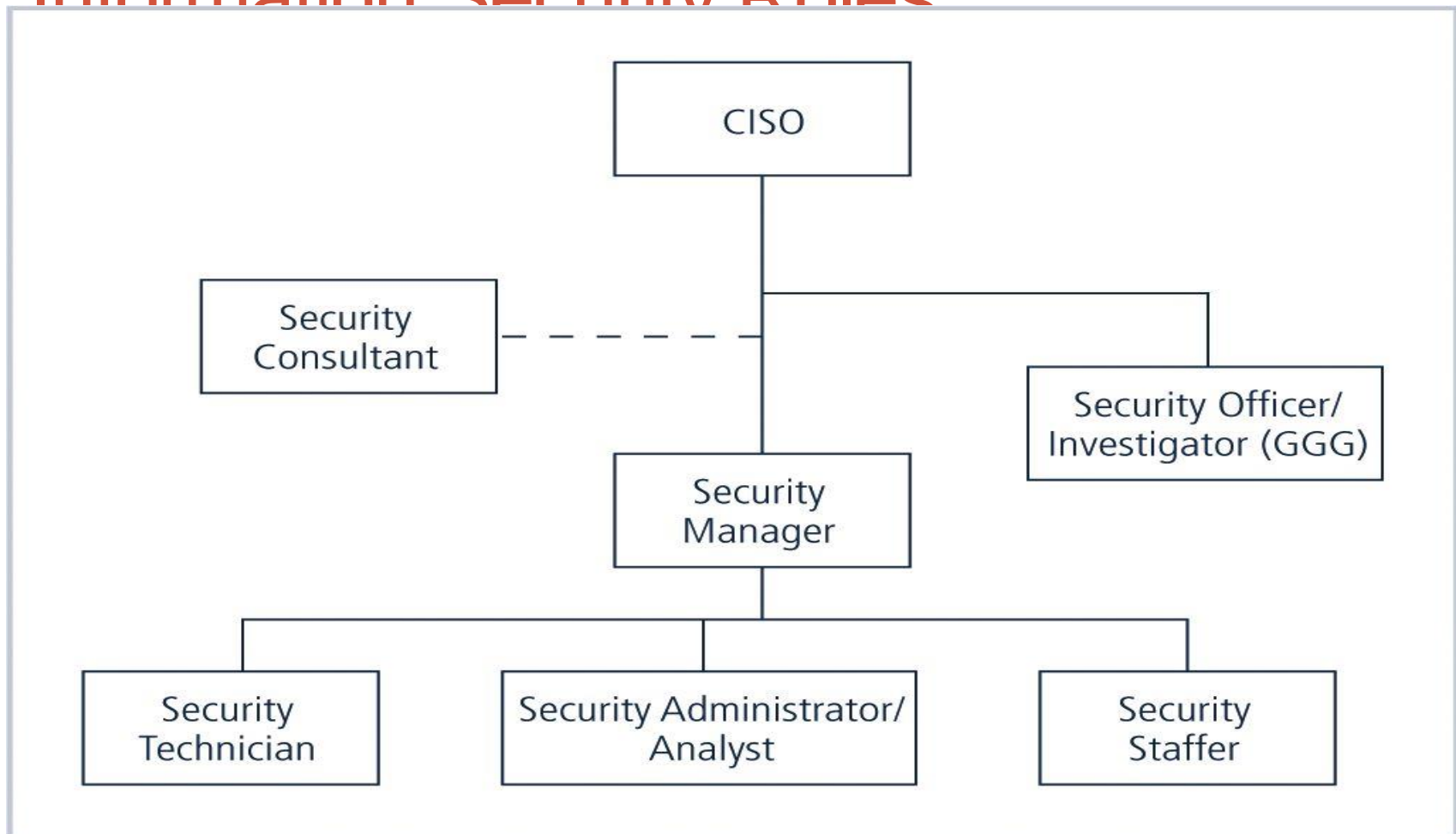


FIGURE 5-11 Information Security Roles

Integrating Security and the Help Desk

- Help desk is an important part of the information security team, enhancing the ability to identify potential problems
- When a user calls help desk with a complaint about his or her computer, the network, or an Internet connection, the user's problem may turn out to be related to a bigger problem, such as a hacker, denial-of-service attack, or a virus
- Because help desk technicians perform a specialized role in information security, they have a need for specialized training

Implementing Security Education, Training, and Awareness Programs

- SETA program: designed to reduce accidental security breaches
- Awareness, training, and education programs offer two major benefits:
 - Improve employee behavior
 - Enable organization to hold employees accountable for their actions
- SETA program consists of three elements: security education, security training, and security awareness

Implementing Security Education, Training, and Awareness Programs (Continued)

- The purpose of SETA is to enhance security:
 - By building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems
 - By developing skills and knowledge so that computer users can perform their jobs while using IT systems more securely
 - By improving awareness of the need to protect system resources

Comparative SETA Framework

	AWARENESS	TRAINING	EDUCATION
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Objective:	Recognition	Skill	Understanding
Teaching Method:	<u>Media</u> - Videos -Newsletters -Posters, etc.	<u>Practical Instruction</u> - Lecture - Case study workshop - Hands-on practice	<u>Theoretical Instruction</u> - Discussion Seminar - Background reading
Test Measure:	True/False Multiple Choice (identify learning)	Problem Solving (apply learning)	Eassay (interpret learning)
Impact Timeframe:	Short-term	Intermediate	Long-term

Security Training

- Security training involves providing detailed information and hands-on instruction to give skills to users to perform their duties securely
- Two methods for customizing training
 - Functional background:
 - General user
 - Managerial user
 - Technical user
 - Skill level:
 - Beginner
 - Intermediate
 - Advanced

Training Techniques

- Using wrong method can:
 - Delay transfer of knowledge
 - Lead to unnecessary expense and frustrated, poorly trained employees
- Good training programs:
 - Use latest learning technologies and best practices
 - Recently, less use of centralized public courses and more on-site training
 - Often for one or a few individuals, not necessarily for large group → waiting for large-enough group can cost companies productivity
 - Increased use of short, task-oriented modules and training sessions that are immediate and consistent, available during normal work week

Delivery Methods

- Selection of training delivery method:
 - Not always based on best outcome for the trainee
 - Other factors: budget, scheduling, and needs of the organization often come first
 - One-on-One
 - Formal Class
 - Computer-Based Training (CBT)
 - Distance Learning/Web Seminars
 - User Support Group
 - On-the-Job Training
 - Self-Study (Noncomputerized)

Selecting the Training Staff

- Employee training:
 - Local training program
 - Continuing education department
 - External training agency
 - Professional trainer, consultant, or someone from accredited institution to conduct on-site training
 - In-house training using organization's own employees

Implementing Training

- While each organization develops its own strategy based on the techniques discussed above, the following seven-step methodology generally applies:
 - Step 1: Identify program scope, goals, and objectives
 - Step 2: Identify training staff
 - Step 3: Identify target audiences
 - Step 4: Motivate management and employees
 - Step 5: Administer the program
 - Step 6: Maintain the program
 - Step 7: Evaluate the program

Security Awareness

- Security awareness program: one of least frequently implemented, but most effective security methods
- Security awareness programs:
 - Set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure
 - Remind users of the procedures to be followed

SETA Best Practices

- When developing an awareness program:
 - Focus on people
 - Refrain from using technical jargon
 - Use every available venue
 - Define learning objectives, state them clearly, and provide sufficient detail and coverage
 - Keep things light
 - Don't overload the users
 - Help users understand their roles in InfoSec
 - Take advantage of in-house communications media
 - Make the awareness program formal; plan and document all actions
 - Provide good information early, rather than perfect information late

The Ten Commandments of InfoSec Awareness Training

- Information security is a people, rather than a technical, issue
- If you want them to understand, speak their language
- If they cannot see it, they will not learn it
- Make your point so that you can identify it and so can they
- Never lose your sense of humor
- Make your point, support it, and conclude it
- Always let the recipients know how the behavior that you request will affect them
- Ride the tame horses
- Formalize your training methodology
- Always be timely, even if it means slipping schedules to include urgent information

Employee Behavior and Awareness

- Security awareness and security training are designed to modify any employee behavior that endangers the security of the organization's information
- Security training and awareness activities can be undermined, however, if management does not set a good example

Employee Accountability

- Effective training and awareness programs make employees accountable for their actions
- Dissemination and enforcement of policy become easier when training and awareness programs are in place
- Demonstrating due care and due carefulness can insure the institution against lawsuits

Awareness Techniques

- Awareness can take on different forms for particular audiences
- A security awareness program can use many methods to deliver its message
- Effective security awareness programs need to be designed with the recognition that people tend to practice a tuning out process (acclimation)
 - Awareness techniques should be creative and frequently changed

Developing Security Awareness Components

- Many security awareness components are available at little or no cost - others can be very expensive if purchased externally
- Security awareness components include the following:
 - Videos
 - Posters and banners
 - Lectures and conferences
 - Computer-based training
 - Newsletters
 - Brochures and flyers
 - Trinkets (coffee cups, pens, pencils, T-shirts)
 - Bulletin boards

The Security Newsletter

- Security newsletter: cost-effective way to disseminate security information
 - In the form of hard copy, e-mail, or intranet
 - Topics can include threats to the organization's information assets, schedules for upcoming security classes, and the addition of new security personnel
- Goal: keep information security uppermost in users' minds and stimulate them to care about security

The Security Newsletter (Continued)

- Newsletters might include:
 - Summaries of key policies
 - Summaries of key news articles
 - A calendar of security events, including training sessions, presentations, and other activities
 - Announcements relevant to information security
 - How-to's

The Security Poster

- Security poster series can be a simple and inexpensive way to keep security on people's minds
- Professional posters can be quite expensive, so in-house development may be best solution
- Keys to a good poster series:
 - Varying the content and keeping posters updated
 - Keeping them simple, but visually interesting
 - Making the message clear
 - Providing information on reporting violations

Figure 5-15

Security Posters

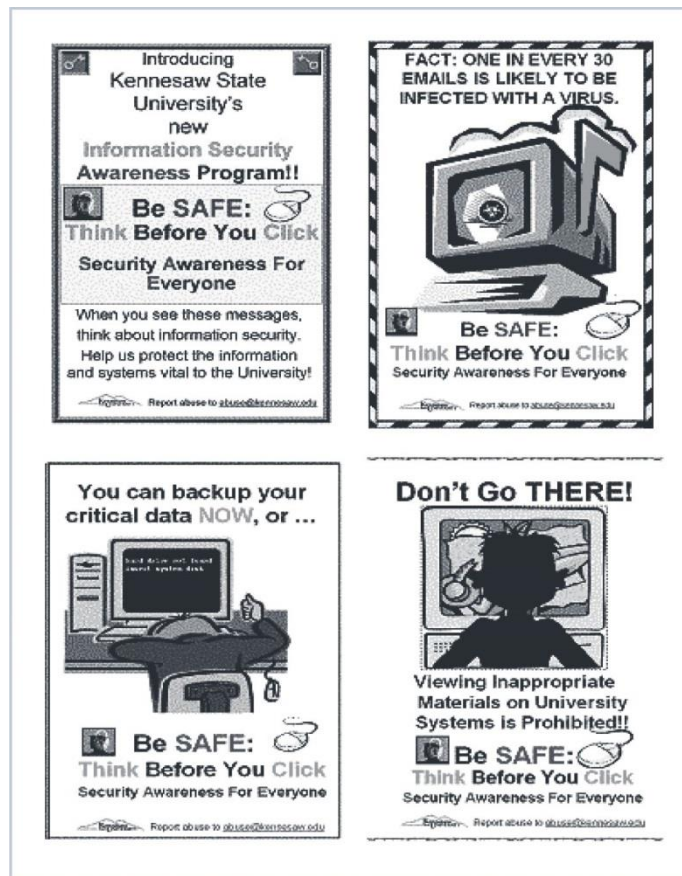


FIGURE 5-15 SETA Awareness Components: Posters

The Trinket Program

- Trinkets may not cost much on a per-unit basis, but they can be expensive to distribute throughout an organization
- Several types of trinkets are commonly used:
 - Pens and pencils
 - Mouse pads
 - Coffee mugs
 - Plastic cups
 - Hats
 - T-shirts

Figure 5-16

Security Trinkets



FIGURE 5-16 SETA Awareness Components: Trinkets

Information Security Awareness Web Site

- Organizations can establish Web pages or sites dedicated to promoting information security awareness
- As with other SETA awareness methods, the challenge lies in updating the messages frequently enough to keep them fresh

Information Security Awareness Web Site (Continued)

- Some tips on creating and maintaining an educational Web site are provided here:
 - See what's already out there
 - Plan ahead
 - Keep page loading time to a minimum
 - Seek feedback
 - Assume nothing and check everything
 - Spend time promoting your site

Security Awareness Conference/Presentations

- Another means of renewing the information security message is to have a guest speaker or even a mini-conference dedicated to the topic
- Perhaps in association with National Computer Security Day - November 30

Summary

- Components of the Security Program
- Information Security Roles and Titles
- Implementing Security Education, Training, and Awareness Programs