# Management of Information Security, 4th Edition

*Chapter 5*

*Developing the Security Program*

# Objectives

- Explain the organizational approaches to information security
- List and describe the functional components of an information security program
- Discuss how to plan and staff an organization’s information security program based on its size
- Describe the internal and external factors that influence the activities and organization of an information security program

# Objectives (continued)

- List and describe the typical job titles and functions performed in the information security program
- Discuss the components of a security education, training, and awareness program and explain how organizations create and manage these programs

# Organizing for Security

- Variables that determine how an organization chooses to structure its information security (InfoSec) program are:
  - Organizational culture, size, security personnel budget, and security capital budget
- An organization's size and available resources directly affect the size and structure of its InfoSec

# Organizing for Security (continued)

- Personnel budget for InfoSec is also a factor
- Another important variable is the portion of capital and expense budget for physical resources that is dedicated to InfoSec
  - Includes allocation of offices, computer labs, and testing facilities

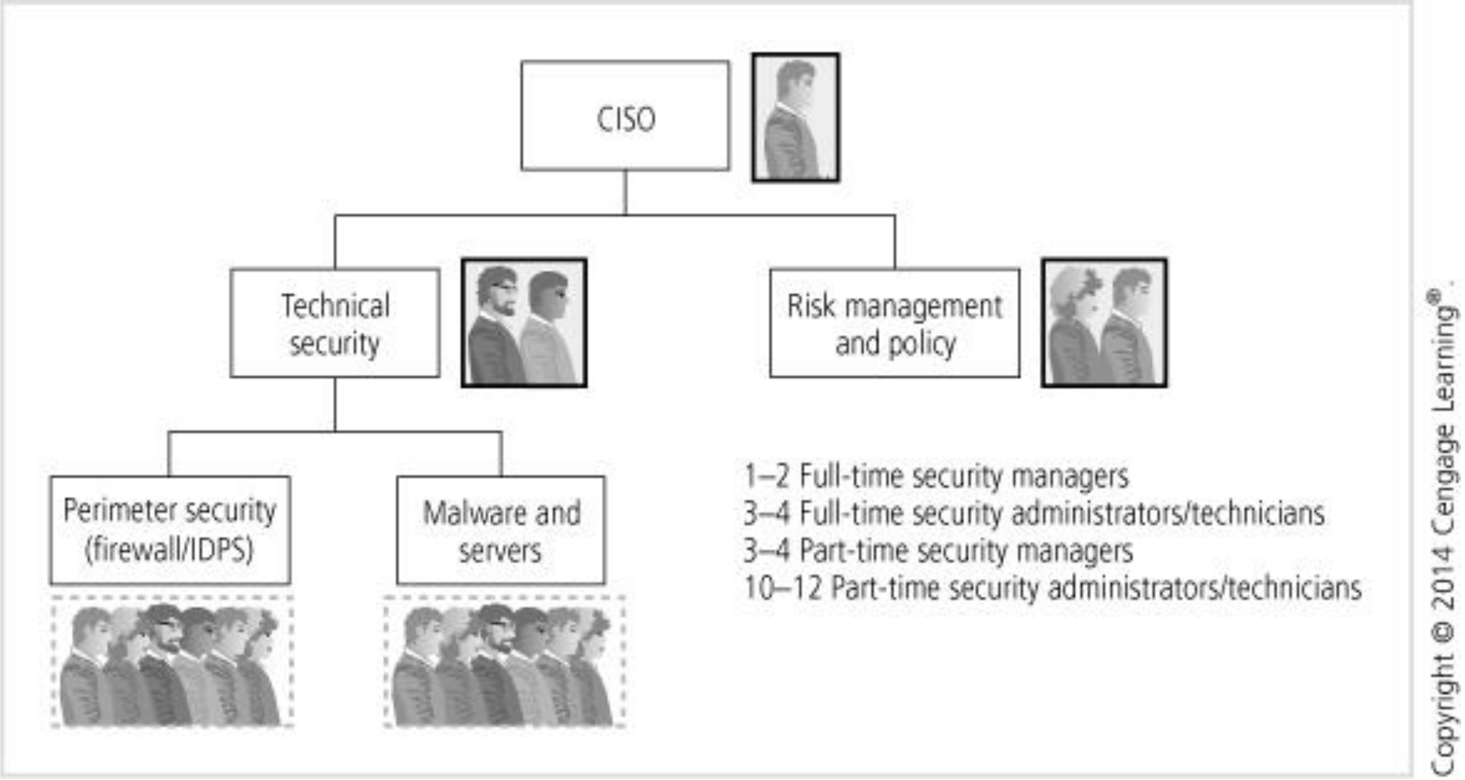
# Security in Large Organizations

- Organizations that have more than 1000 devices and require security management
  - Are likely to be staffed and funded at a level that enables them to accomplish most InfoSec functions
- A recommended approach is to separate the functions into four areas
  - Functions performed by non technology business units outside IT
    - Legal, training
  - Functions performed by IT groups outside InfoSec
    - Systems and network security administration

# Security in Large Organizations (continued)

- A recommended approach is to separate the functions into four areas (cont'd)
  - Functions performed within the InfoSec department as a customer service to the organization:
    - Risk assessment, systems testing, incident response
  - Functions performed within the InfoSec department as a compliance enforcement obligation
    - Policy, compliance/audit, risk management
- It remains the CISO's responsibility to see that InfoSec functions are adequately performed within the organization

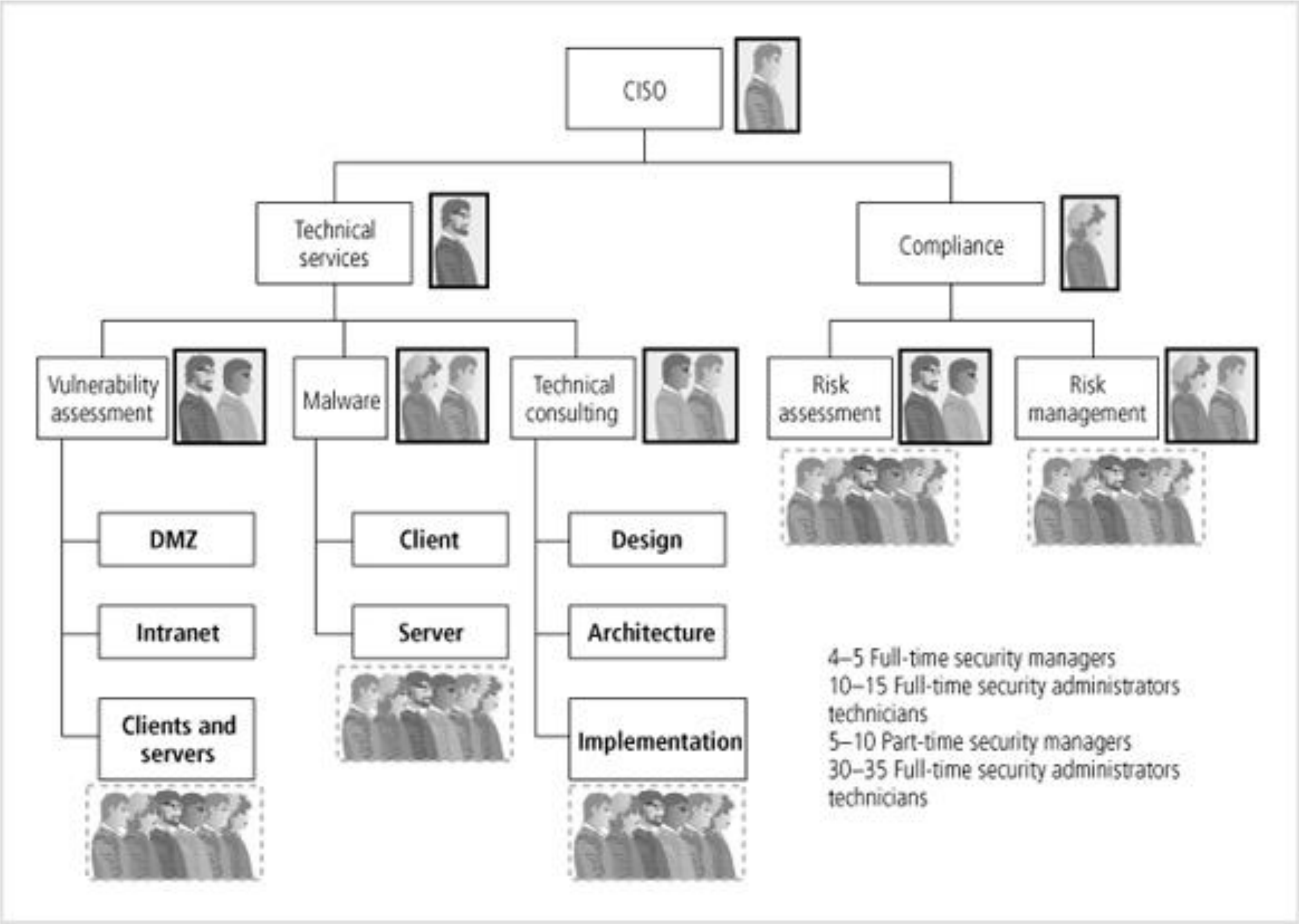
# **Figure 5-1** Example of InfoSec staffing in a large organization


CISO
Technical security
Risk management and policy
Perimeter security (firewall/IDPS)
Malware and servers

1–2 Full-time security managers
3–4 Full-time security administrators/technicians
3–4 Part-time security managers
10–12 Part-time security administrators/technicians

Copyright © 2014 Cengage Learning®.

# **Figure 5-2** Example of InfoSec staffing in a very large organization

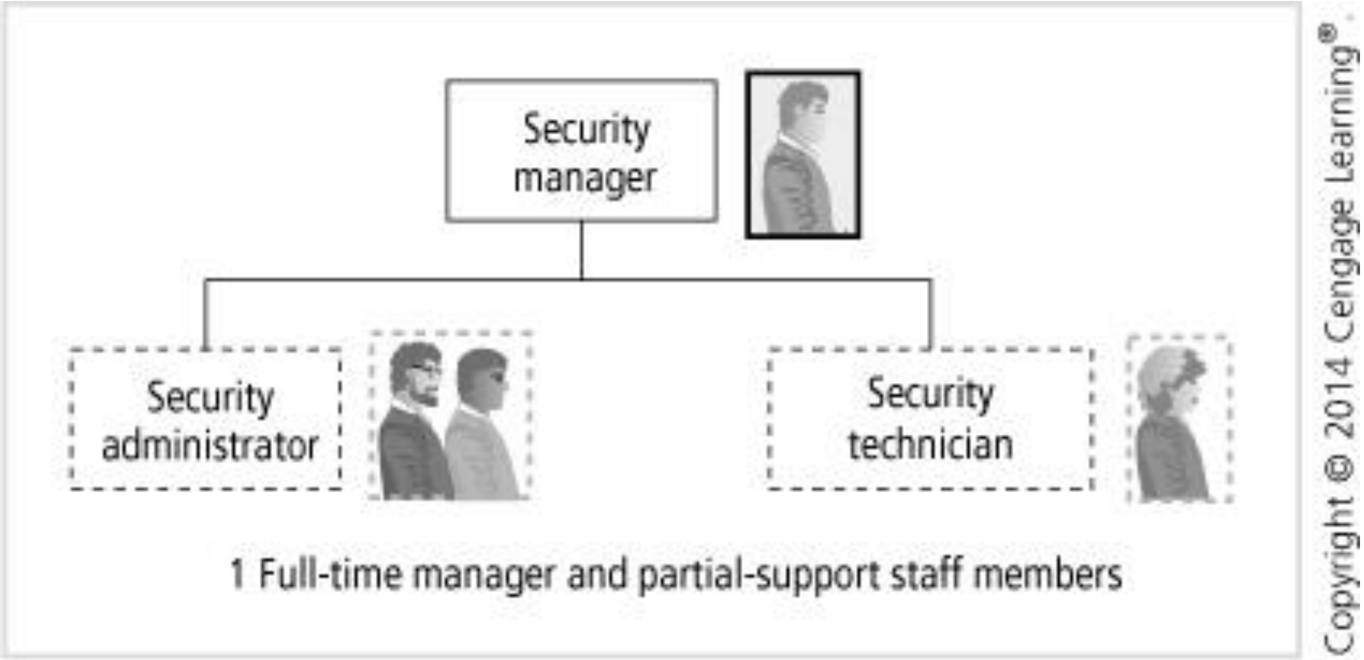


Copyright © 2014 Cengage Learning®

# Security in Medium-Sized Organizations

- Medium-sized organizations have between 100 and 1000 machines requiring security management
  - May still be large enough to implement the multi-tiered approach to security
- Medium-sized organizations tend to ignore some of the InfoSec functions
  - When they cannot staff a certain function
  - The CISO must improve collaboration among InfoSec and IT departments

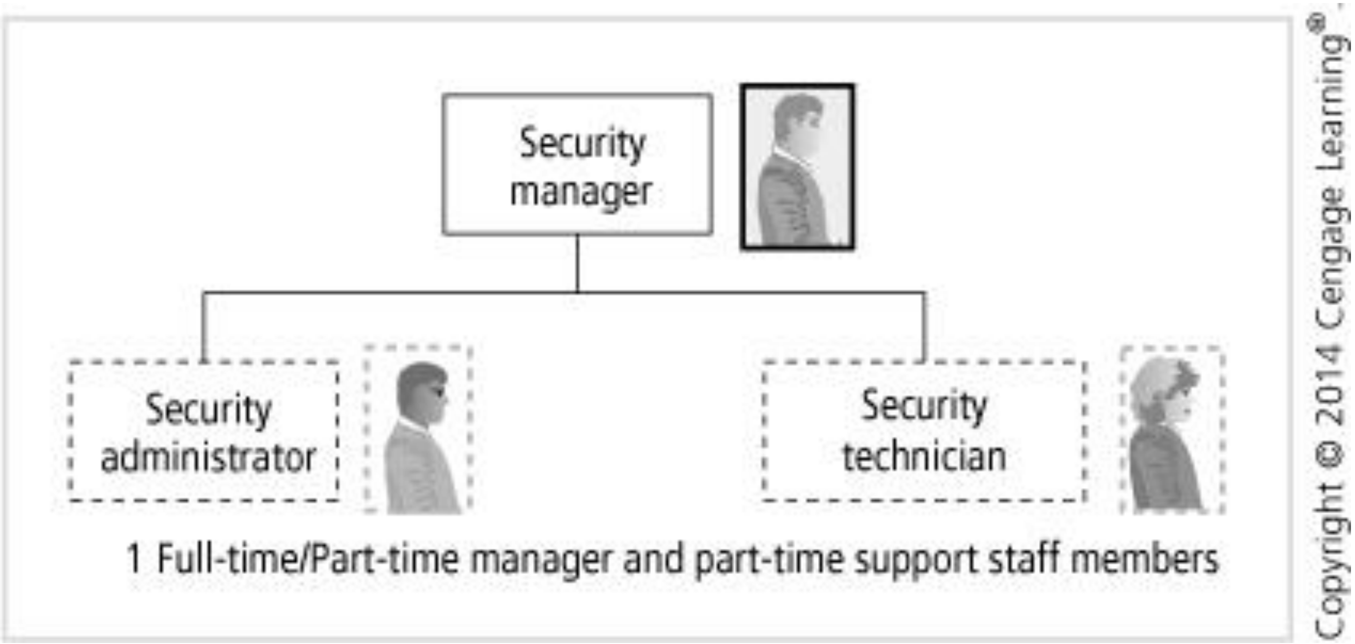
# **Figure 5-3** Example of InfoSec staffing in a medium-sized organization


Security manager
Security administrator
Security technician
1 Full-time manager and partial-support staff members
Copyright © 2014 Cengage Learning®.

# Security in Small Organizations

- Smaller organizations - fewer than 100 systems
  - InfoSec often becomes the responsibility of a single security administrator
- Smaller organizations typically have minimal formal policy, planning, or security measures
- Security administrators may use freeware or open source software to lower costs of security
- Threats from insiders are less likely

# **Figure 5-4** Example of InfoSec staffing in a smaller organization


Security manager
Security administrator
Security technician
1 Full-time/Part-time manager and part-time support staff members
Copyright © 2014 Cengage Learning®

# Placing Information Security within an Organization

- In large organizations:
  - The InfoSec department may be located within an IT division headed by the CISO, who reports to CIO
- Operating an InfoSec program within an IT division
  - May cause InfoSec goals and objectives to contradict those of the IT division as a whole
- Goals and objectives of the CIO and CISO may come in conflict

# Components of the Security Program

- The CIO and CISO should use these two documents to formulate the mission statement for the InfoSec program
- An informative NIST publication:
  - SP 80012, An Introduction to Computer Security: The NIST Handbook

# Components of the Security Program (continued)

- The “NIST Handbook” covers the following topics:
  - Elements of computer security
  - Roles and responsibilities
  - Common threats
  - Common InfoSec controls
  - Risk management
  - Security program management
  - Contingency planning

# **Table 5-2** Elements of a security program

| Primary Element | Components |
|---|---|
| Policy | Program policy, issue-specific policy, system-specific policy |
| Program management | Central security program, system-level program |
| Risk management | Risk assessment, risk mitigation, uncertainty analysis |
| Life cycle planning | Security plan, initiation phase, development/acquisition phase, implementation phase, operation/maintenance phase |
| Personnel/user issues | Staffing, user administration |
| Preparing for contingencies and disaster? | Business plan, identify resources, develop scenarios, develop strategies, test |
| Computer security incident handling | Incident detection, reaction, recovery, and follow-up |
| Awareness and training | SETA plans, awareness projects, and policy and procedure training |
| Security considerations in computer support and operations | Help desk integration, defending against social engineering, and improving system administration |
| Physical and environmental security | Guards, gates, locks and keys, and alarms |
| identification and authentication | Identification, authentication, passwords, advanced authentication |
| Logical access control | Access criteria, access control mechanisms |
| Audit trails | System logs, log review processes, and log consolidation and management |
| Cryptography | TKI. VPN. key management, and key recovery |

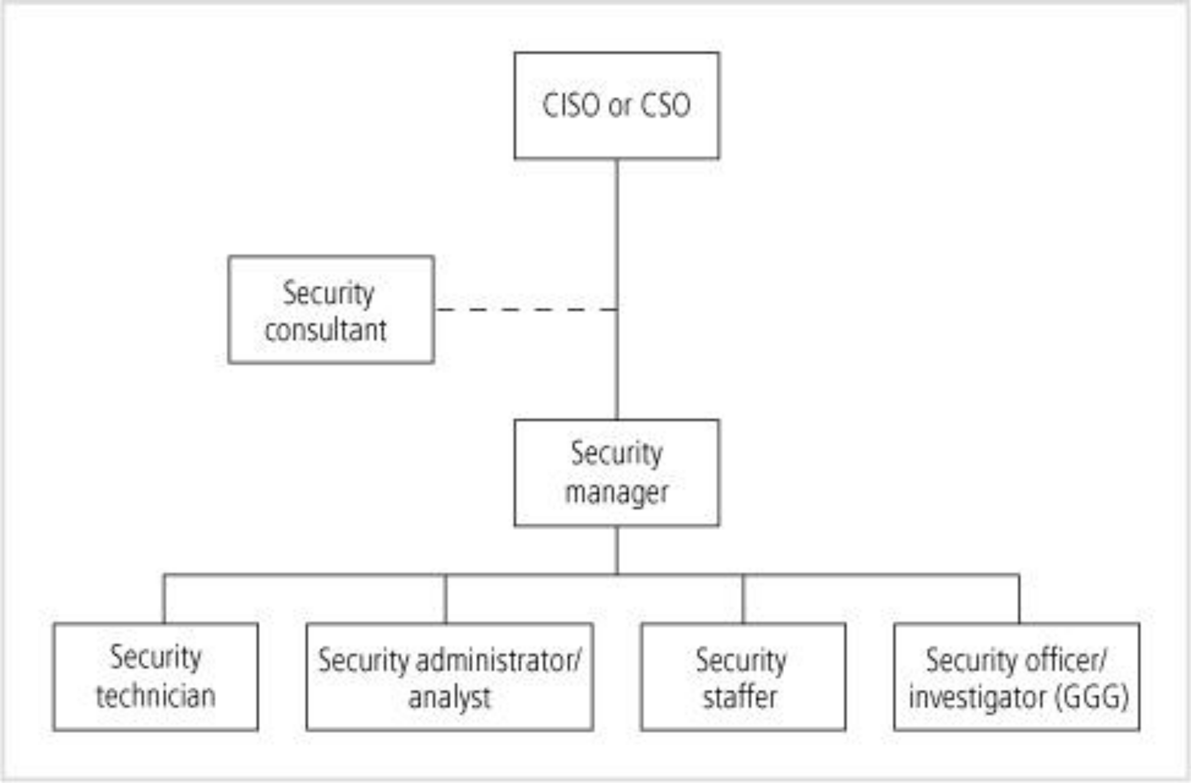
# Information Security Roles and Titles Part 1

- InfoSec positions can be classified into three types:
  - Those that define
  - Those that build
  - Those that administer
- A typical organization has a number of individuals with InfoSec responsibilities

# Information Security Roles and Titles Part 2

- **Chief Information Security Officer (CISO)**
  - Primarily responsible for the assessment, management, and implementation of the program that secures the organization's information
  - May also be called chief security officer (CSO)

# **Figure 5-10** InfoSec roles



Copyright © 2014 Cengage Learning®.

# Information Security Roles and Titles Part 3

- **Security Managers** - accountable for the day-to-day operations of the InfoSec program
  - Accomplish objectives set by the CISO
  - Resolve issues identified by technicians, administrators, analysts, or staffers

# Information Security Roles and Titles Part 4

- **Security Administrators and Analysts**
  - Security administrators are a hybrid of a security technician and a security manager
  - Security analysts are a specialized security administrator

# Information Security Roles and Titles Part 6

- **Security Technicians** - configure firewalls and IDPSs, implement security software, diagnose and troubleshoot problems, and coordinate with systems and network administrators to ensure security technology is properly implemented

# Information Security Roles and Titles Part 7

- **Security Staffers and Watchstanders**
  - Security staffer - individuals who perform routine administrative activities
  - Watchstanders - watch intrusion controls, monitor e-mail accounts, and perform routine security roles

# Information Security Roles and Titles Part 8

- **Security Consultants** - typically an independent expert in some aspect of InfoSec
  - Brought in as an outsource

# Information Security Roles and Titles Part 9

- **Security Officers and Investigators**
  - These roles are often closely related to law enforcement and/or criminal justice

# Information Security Roles and Titles Part 10

- **Help Desk Personnel**
  - The help desk enhances the security team's ability to identify potential problems
  - Must be prepared to identify and diagnose traditional and technical problems and threats to InfoSec

# Implementing Security Education, Training, and Awareness Programs

- **Security, education, training, and awareness (SETA)** program is the responsibility of the CISO
  - Is designed to reduce the incidence of accidental security breaches by members of the organization
- SETA programs offer three benefits:
  - Can improve employee behavior
  - Can inform members of the organization about where to report violations of policy
  - Enable the organization to hold employees accountable for their actions

# Implementing Security Education, Training, and Awareness Programs (continued)

- SETA programs enhance general education and training programs by focusing on InfoSec
- A SETA program consists of three elements: security education, security training, and security awareness
- SETA enhances security by:
  - Building in-depth knowledge to design, implement, or operate security programs
  - Developing skills and knowledge
  - Improving awareness of the need to protect systems

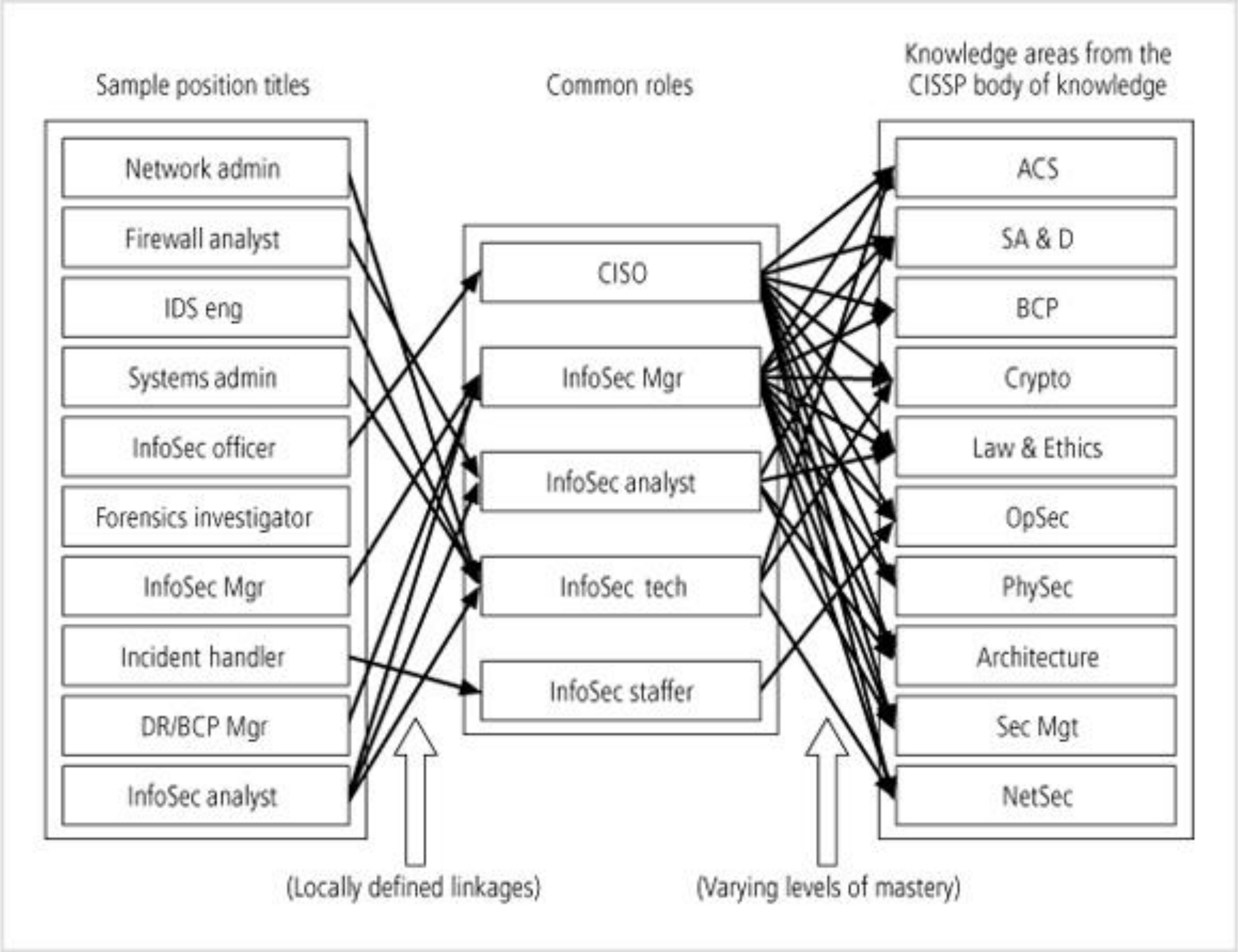
# **Table 5-3** Framework of security education, training, and awareness

| | Awareness | Training | Education |
|---|---|---|---|
| Attribute | Seeks to teach members of the organization what security is and what the employee should do in some situations. | Seeks to train members of the organization how they should react and respond when threats are encountered in specified situations. | Seeks to educate members of the organization as to why the organization has prepared in the way that it has and why the organization reacts in the ways that it does- |
| Level | Offers basic information about threats and responses. | Offers more detailed knowledge about detecting threats and teaches skills needed for effective reaction. | Offers the background and depth of knowledge to gain insight into how processes are developed and enables ongoing improvement. |
| Objective | Members of the organization can recognize threats and formulate simple responses. | Members of the organization can mount effective responses using learned skills. | Members of the organization can engage in active defense and use understanding of the organizations objectives to make continuous improvement. |
| Teaching methods | • Media videos<br>• Newsletters<br>• Posters<br>• Informal training | • Formal training<br>• Workshops<br>• Hands-on practice | • Theoretical instruction<br>• Discussions/seminars<br>• Background reading |
| Assessment | True/False or Multiple Choice (Identify learning) | Problem solving (apply learning) | Essay (interpret learning) |
| Impact timeframe | Short-term | Intermediate | Long-term |

# Security Education

- InfoSec training programs must address the following issues:
  - The InfoSec educational components required of all InfoSec professionals
  - The general educational requirements that all IT professionals must have
- A number of colleges and universities provide formal coursework in InfoSec

# **Figure 5-11** InfoSec knowledge map



Copyright © 2014 Cengage Learning®.

© Cengage Learning 2014

# Security Training Part 1

- Security training - providing members of the organization with detailed information and hands-on instruction
  - To enable them to perform their duties securely
- Training may include: custom in-house training developed by InfoSec management
  - Or outsource all or part of the training program
- A resource to help organizations put together SETA programs:
  - The Computer Security Resource Center at NIST

# Security Training Part 2

- **Training for Technical Users** - more detailed than user or managerial training
- Three methods for developing advanced technical training:
  - By job category
    - Technical users versus managers
  - By job function
    - Accounting versus marketing
  - By technology product
    - E-mail client, database

# Security Training Part 3

- **Training for General Users** - a method of ensuring policies are read and understood by general users is to provide training on those policies
  - Allows the organization to collect the required letters of compliance
  - Employee orientation is a good time to conduct it

# Security Training Part 4

- **Training for Managerial Users** - managers typically expect a more personal form of training
  - With smaller groups and more interaction
  - Support at executive level can convince managers to attend training events

# Training Techniques

- **Delivery Methods** - selection of the delivery method is not always based on the best outcome for the trainee
  - Budget, scheduling, and needs of organization can come first
- **Selecting the Training Staff** - An organization can use:
  - A local training program, a continuing education department, or an external training agency
  - Can also organize and conduct in-house training using its own employees

# **Table 5-4** Training delivery methods

| Method | Advantages | Disadvantages |
|---|---|---|
| One-on-one: A dedicated trainer works with each trainee on the areas specified. | • Informal<br>• Personal<br>• Customized to the needs of the trainee<br>• Can be scheduled to fit the needs of the trainee | • Resource intensive, to the point of being inefficient |
| Formal class: A tingle trainer works with multiple trainees in a formal setting | • Formal training plan, efficient<br>• Trainees able to learn from each other<br>• Interaction possible with trainer<br>• Usually considered cost-effective | • Relatively inflexible<br>• May not be sufficiently responsive to the needs of all trainees<br>• Difficult to schedule, especially if more than one session is needed |
| Computer-based training (CBT): Prepackaged software that provides training at the trainees workstation. | • Flexible, no special scheduling requirements<br>• Self-paced, can go as fast or as slow as the trainee needs<br>• Can be very cost-effective | • Software can be very expensive.<br>• Content may not be customized to the needs of the organization |
| Distance learning/Web seminars: Trainees receive a seminar presentation at their computers. Some models allow teleconferencing for voice feedback; others have text questions and feedback. | • Can be live or can be archived and viewed at the trainee's convenience<br>• Can be low or no-cost | • If archived, can be very inflexible, with no mechanism for trainee feedback |
| User support group: Support from a community of users is commonly facilitated by a particular vendor as a mechanism to augment the support for products or software | • Allows users to learn from each other<br>• Usually conducted in an informal social setting | • Does not use a formal training model<br>• Centered on a specific topic or product |
| On-the-job training: Trainees learn the specifics of their jobs while working, using the software, hardware, and procedures they will continue to use. | • Very applied to the task at hand<br>• inexpensive | • A sink-or-swim approach<br>• Can result in substandard work performance until trainee gets up to speed |
| Self-Study (noncomputerized): Trainees study materials on their own. usually when not actively performing their Jobs. | • Lowest cost to the organization<br>• Places materials in the hands of the trainee<br>• Trainees can select the material they need to focus on the most<br>• Self-paced | • Shifts responsibility for training onto the trainee, with little formal support |

# Training Techniques (continued)

- Implementing Training - Each organization develops it own strategy but the following seven-step methodology can apply:
  - Identify program, scope, goals, and objectives
  - Identify training staff
  - Identify target audiences
  - Motivate management and employees
  - Administer the program
  - Maintain the program
  - Evaluate the program

# Security Awareness

- When developing an awareness program:
  - Focus on  people both as part of the problem and part of the solution
  - Define at least one key learning objective, state it clearly, and provide sufficient detail and coverage to reinforce the learning of it

# Security Awareness (continued)

- When developing an awareness program (cont’d):
  - Do not overload users with too much detail
  - Help users understand their roles in InfoSec and how a breach in security can affect their jobs
  - Take advantage of in-house communications media to deliver messages
  - Make the awareness program formal
  - Provide good information early, rather than perfect information late

# Advice for Information Security Awareness Training Programs

- Observations about SETA training practices:
  - Information security is about people and only incidentally related to technology
  - If you want others to understand, learn how to speak a language they can understand
  - If they don’t understand, they will not be able to learn

# Advice for Information Security Awareness Training Programs (continued)

- Observations about SETA training practices (cont’d):
  - Unambiguously tell students how the behavior you request will affect them as well as how failure to conform to that behavior will affect them
  - Continue to train with information about problems and solutions for those issues that have already been resolved
  - Formalize your training methodology until it is a repeatable process
  - Always be timely

# Employee Behavior and Awareness

- By teaching employees how to properly handle information, use applications, and operate within the organization

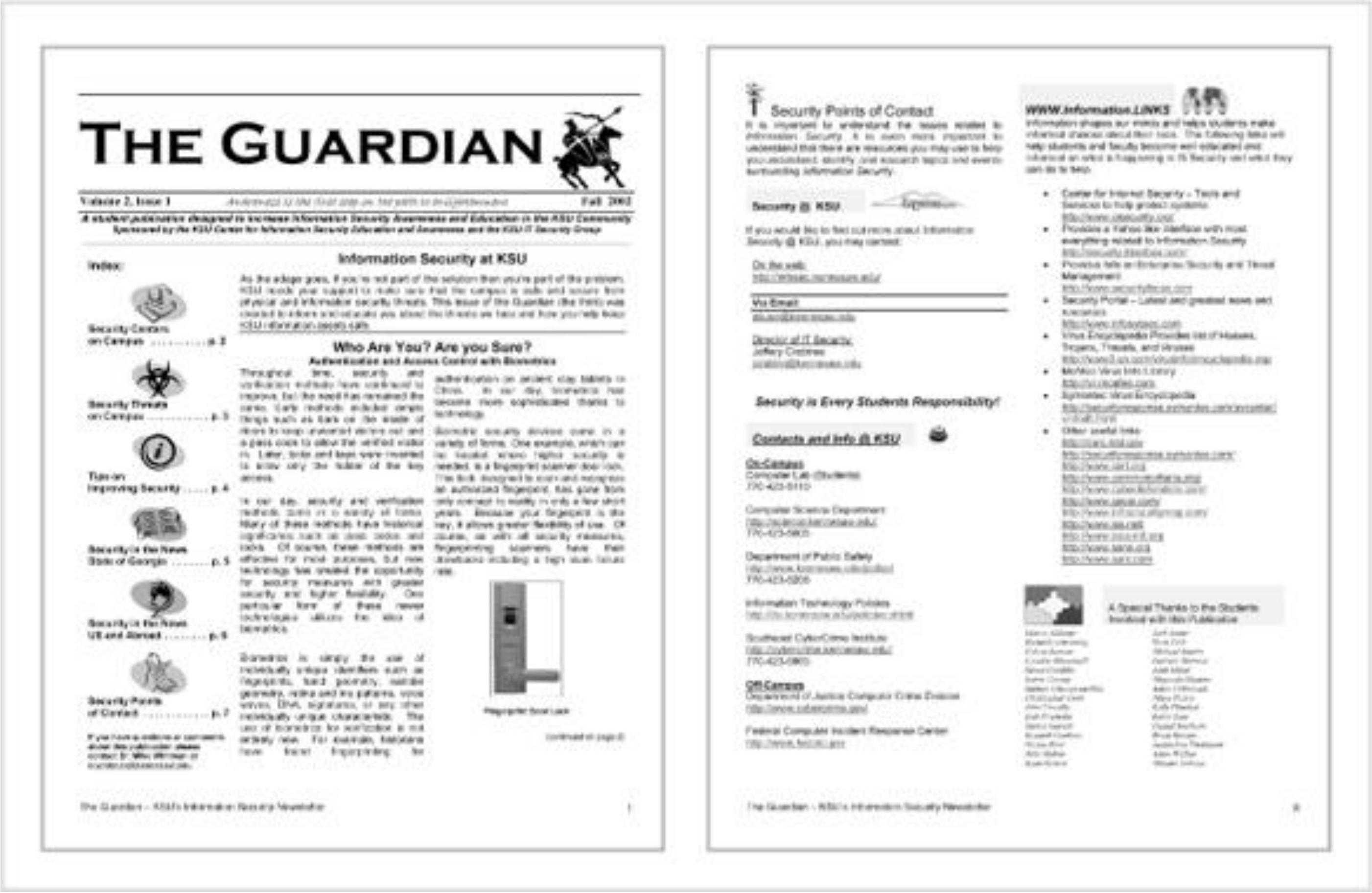
# Developing Security Awareness Components Part 1

- Security awareness components include:
  - Videos
  - Posters and banners
  - Lectures and conferences
  - Computer-based training
  - Newsletters
  - Brochures and flyers
  - Trinkets (coffee cups, pens, pencils, T-shirts)
  - Bulletin boards

# Developing Security Awareness Components Part 2

- ***Security Newsletter*** - most cost-effective method of disseminating security information and news to employees
  - Via hard copy, e-mail, or intranet
- A few things it might include:
  - Summaries of key policies
  - Summaries of key news articles
  - Calendar of security events
  - Announcements relevant to InfoSec
  - How-to articles

# **Figure 5-13** SETA awareness components: newsletters



# THE GUARDIAN

Volume 2, Issue 1 — [illegible] — Fall 2002

*A student publication designed to increase Information Security Awareness and Education in the KSU Community*
*Sponsored by the KSU Center for Information Security Education and Awareness and the KSU IT Security Group*

Index:

Security Centers on Campus ............ p. 2

Security Threats on Campus ............ p. 3

Tips on Improving Security ...... p. 4

Security in the News State of Georgia ......... p. 5

Security in the News US and Abroad ......... p. 6

Security Points of Contact ............ p. 7

If you have questions or comments about this publication please contact Dr. [illegible]

## Information Security at KSU

As the adage goes, if you're not part of the solution then you're part of the problem. KSU needs your support to make sure that the campus is safe and secure from physical and information security threats. This issue of the Guardian (the third) was created to inform and educate you about the threats we face and how you help keep KSU information assets safe.

## Who Are You? Are you Sure?

**Authentication and Access Control with Biometrics**

Throughout time, security and verification methods have continued to improve, but the need has remained the same. Early methods included simple things such as bars on the inside of doors to keep unwanted visitors out and a pass code to allow the verified visitor in. Later, locks and keys were invented to allow only the holder of the key access.

In our day, security and verification methods come in a variety of forms. Many of these methods have historical significance such as pass codes and locks. Of course, these methods are effective for most purposes, but new technology has created the opportunity for security measures with greater security and higher flexibility. One particular form of these newer technologies utilizes the idea of biometrics.

Biometrics is simply the use of individually unique identifiers such as fingerprints, hand geometry, facial geometry, retina and iris patterns, voice waves, DNA, signatures, or any other individually unique characteristic. The use of biometrics for verification is not entirely new. For example, historians have traced fingerprinting for authentication on ancient clay tablets in China. In our day, biometrics has become more sophisticated thanks to technology.

Biometric security devices come in a variety of forms. One example, which can be located where higher security is needed, is a fingerprint scanner door lock. The lock designed to scan and recognize an authorized fingerprint, has gone from only concept to reality in only a few short years. Because your fingerprint is the key, it allows greater flexibility of use. Of course, as with all security measures, fingerprinting scanners have their drawbacks including a high false failure rate.

Fingerprint Door Lock

continued on page [illegible]

The Guardian – KSU's Information Security Newsletter 1

## Security Points of Contact

It is important to understand the issues related to Information Security. It is even more important to understand that there are resources you may use to help you understand, identify, and research topics and events surrounding Information Security.

**Security @ KSU**

If you would like to find out more about Information Security @ KSU, you may contact:

On the web:
[illegible]

Via Email:
[illegible]

Director of IT Security:
Jeffery Crabtree
[illegible]

***Security is Every Students Responsibility!***

**Contacts and Info @ KSU**

On-Campus
Computer Lab (Students)
770-423-[illegible]

Computer Science Department
[illegible]
770-423-[illegible]

Department of Public Safety
[illegible]
770-423-[illegible]

Information Technology Policies
[illegible]

Southeast CyberCrime Institute
[illegible]
770-423-[illegible]

Off-Campus
Department of Justice Computer Crime Division
[illegible]

Federal Computer Incident Response Center
[illegible]

**WWW.Information.LINKS**

Information shapes our minds and helps students make informed choices about their lives. The following links will help students and faculty become well educated and informed on what is happening in IS Security and what they can do to help.

- Center for Internet Security – Tools and Services to help protect systems
  http://www.cisecurity.org/
- Provides a Yahoo like interface with most everything related to Information Security
  http://security.itoolbox.com/
- Provides info on Enterprise Security and Threat Management
  http://www.securityfocus.com
- Security Portal – Latest and greatest news and resources
  http://www.infosyssec.com
- Virus Encyclopedia Provides list of Hoaxes, Trojans, Threats, and Viruses
  [illegible]
- McAfee Virus Info Library
  http://vil.mcafee.com
- Symantec Virus Encyclopedia
  [illegible]
- Other useful links
  [illegible]

A Special Thanks to the Students Involved with this Publication

[illegible]

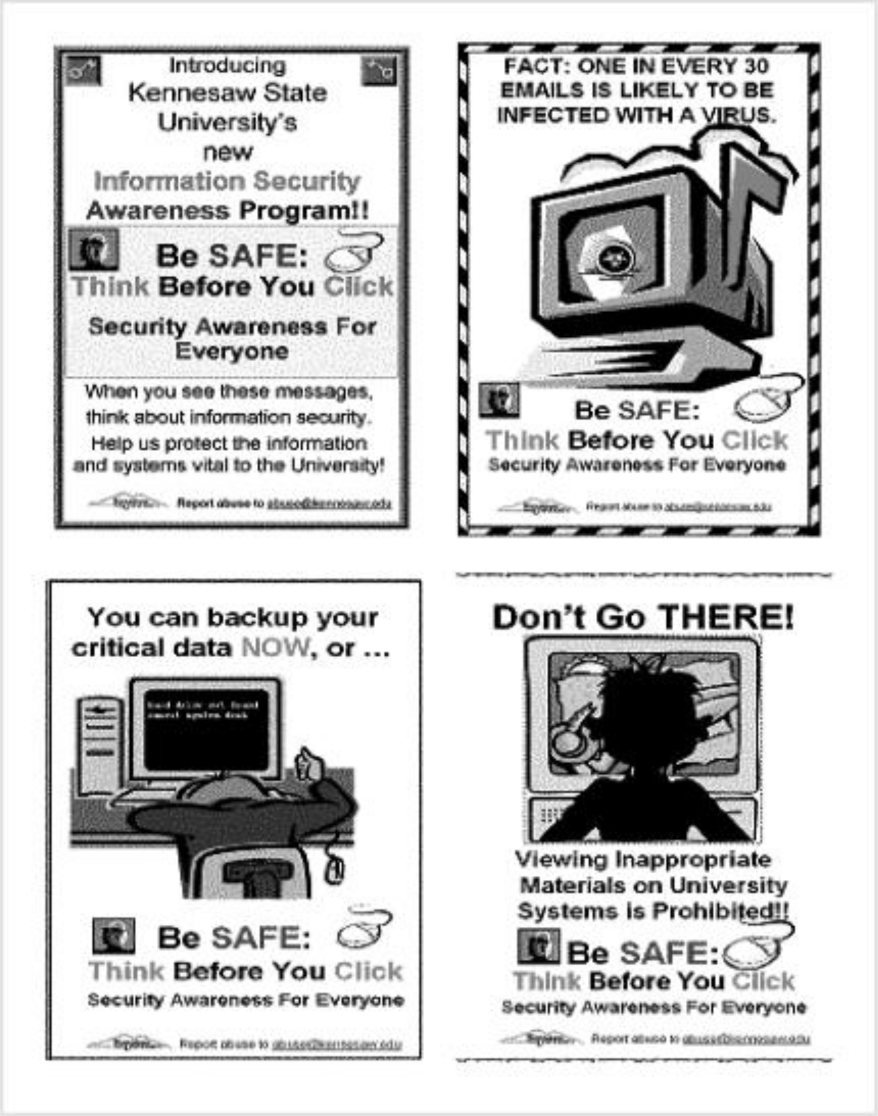
The Guardian – KSU's Information Security Newsletter 8

Copyright © 2014 Cengage Learning®.

# Developing Security Awareness Components Part 3

- ***Security Poster*** - a simple and inexpensive way to keep security on people’s minds
- Several keys to a good poster:
  - Varying the content and keeping posters updated
  - Keeping them simple but visually interesting
  - Making the message clear
  - Providing information on reporting violations

# **Figure 5-14** SETA awareness



Introducing Kennesaw State University's new Information Security Awareness Program!!

Be SAFE: Think Before You Click

Security Awareness For Everyone

When you see these messages, think about information security. Help us protect the information and systems vital to the University!

Report abuse to abuse@kennesaw.edu

FACT: ONE IN EVERY 30 EMAILS IS LIKELY TO BE INFECTED WITH A VIRUS.

Be SAFE: Think Before You Click

Security Awareness For Everyone

Report abuse to abuse@kennesaw.edu

You can backup your critical data NOW, or ...

Be SAFE: Think Before You Click

Security Awareness For Everyone

Report abuse to abuse@kennesaw.edu

Don't Go THERE!

Viewing Inappropriate Materials on University Systems is Prohibited!!

Be SAFE: Think Before You Click

Security Awareness For Everyone

Report abuse to abuse@kennesaw.edu

# Developing Security Awareness Components Part 4

- ***Information Security Awareness Web Site*** - Web pages or sites dedicated to promoting InfoSec awareness
  - When new information is posted, employees can be informed via e-mail
  - May contain the latest and archived newsletters, press releases, awards, and recognitions
  - Recommended to place your Web site on the intranet

# Developing Security Awareness Components Part 5

- ***Security Awareness Conference/Presentations*** - a means of renewing the InfoSec message by having a guest speaker or a mini-conference dedicated to the topic

# Summary

- The term “InfoSec program” is used to describe the structure and organization of the effort that contains risks to the information assets of an organization
- In large organizations, specific InfoSec functions are likely to be performed by specialized groups
  - In smaller organizations, these functions may be carried out by all members of the department
- InfoSec positions can be classified into one of three areas: those that define, those that build, and those that administer
- The SETA program is the responsibility of the CISO

# Summary (continued)

- SETA programs improve employee behavior and enable organizations to hold employees accountable
- Training is most effective when it is designed for a specific category of users
- There are two methods for customizing training for users: by functional background and by level of skill
- A security awareness program can deliver its message via videotapes, newsletters, posters, bulletin boards, flyers, demonstrations, briefings, short reminder notices at log-on, or lectures