CSIT988/CSIT488
Security, Ethics and Professionalism
Week 6: Developing the Security Program

Subject Coordinator: *Dr Khoa Nguyen*

School of Computing and Information Technology

Autumn 2025

Learning 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
- 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 (SETA) program and explain how organizations create and manage these programs

- Some organizations use security program to describe the entire set of personnel, plans, policies, and initiatives related to information security

- The term “information security program” is used here to describe the structure and organization of the effort that contains risks to the information assets of the organization

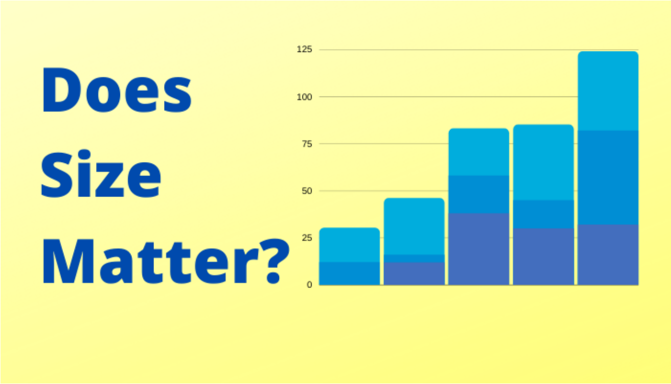
Structuring InfoSec Programs

Variables involved in structuring an InfoSec program

- Organizational culture
- Size
- Personnel budget for the InfoSec program
- Capital and expense budget for InfoSec

"As organizations get larger in size, their security departments are not keeping up with the demands of increasingly complex organizational infrastructures. Security spending per user and per machine declines exponentially as organizations grow."

Briney and Prince, "Does Size Matter?"



Functions Needed to Implement the InfoSec Program

- Risk assessment
- Risk management
- Systems testing
- Policy
- Legal assessment
- Incident response
- Planning

- Measurement
- Compliance
- Centralized authentication
- Systems security administration
- Training
- Network security administration
- Vulnerability assessment

Security in Large Organizations

- InfoSec departments tend to form internal groups
  - To meet long-term challenges and handle day-to-day security operations
- Functions are likely to be split into groups
- Smaller organizations typically create fewer groups

Security in Large Organizations (cont'd.)

One recommended approach separates functions into four areas:

1. Functions performed by non-technology business units outside of IT
   - legal, training

2. Functions performed by IT groups outside of InfoSec area
   - systems, network security administrations, centralized authentication

3. Functions performed within InfoSec department as customer service
   - risk and vulnerability assessments, system testing, IR, planning, measurement

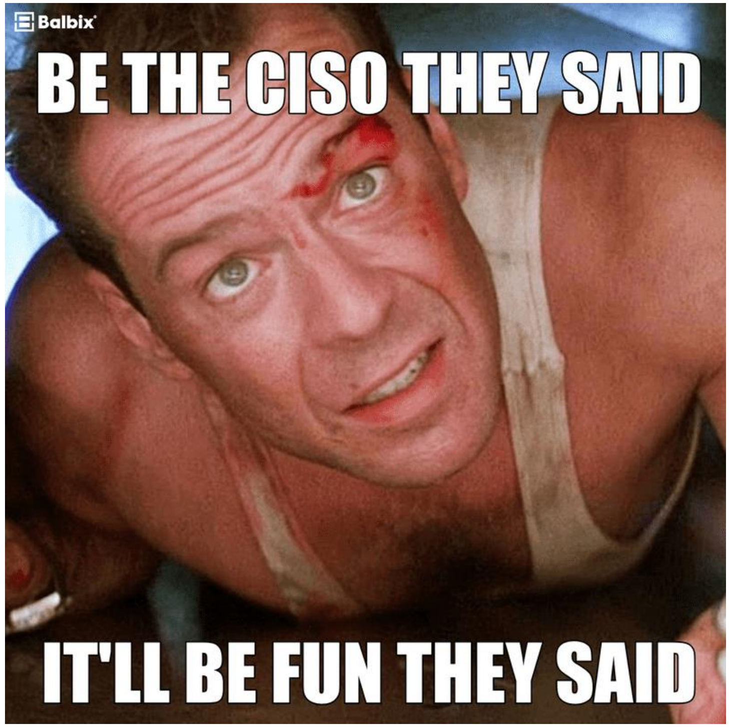
4. Functions performed within the InfoSec department as compliance
   - policy, compliance, risk management

Security in Large Organizations (cont'd.)

- The CISO has responsibility to ensure that InfoSec functions are adequately performed somewhere within the organization

- Large and very large organizations have dedicated staffs to support the security program. The deployment of full-time security personnel depends on many factors:
  - Sensitivity of the information to be protected
  - Industry regulations
  - General profitability

- The more resource the company can dedicate to its personnel budget, the more likely it is to maintain a large InfoSec staff



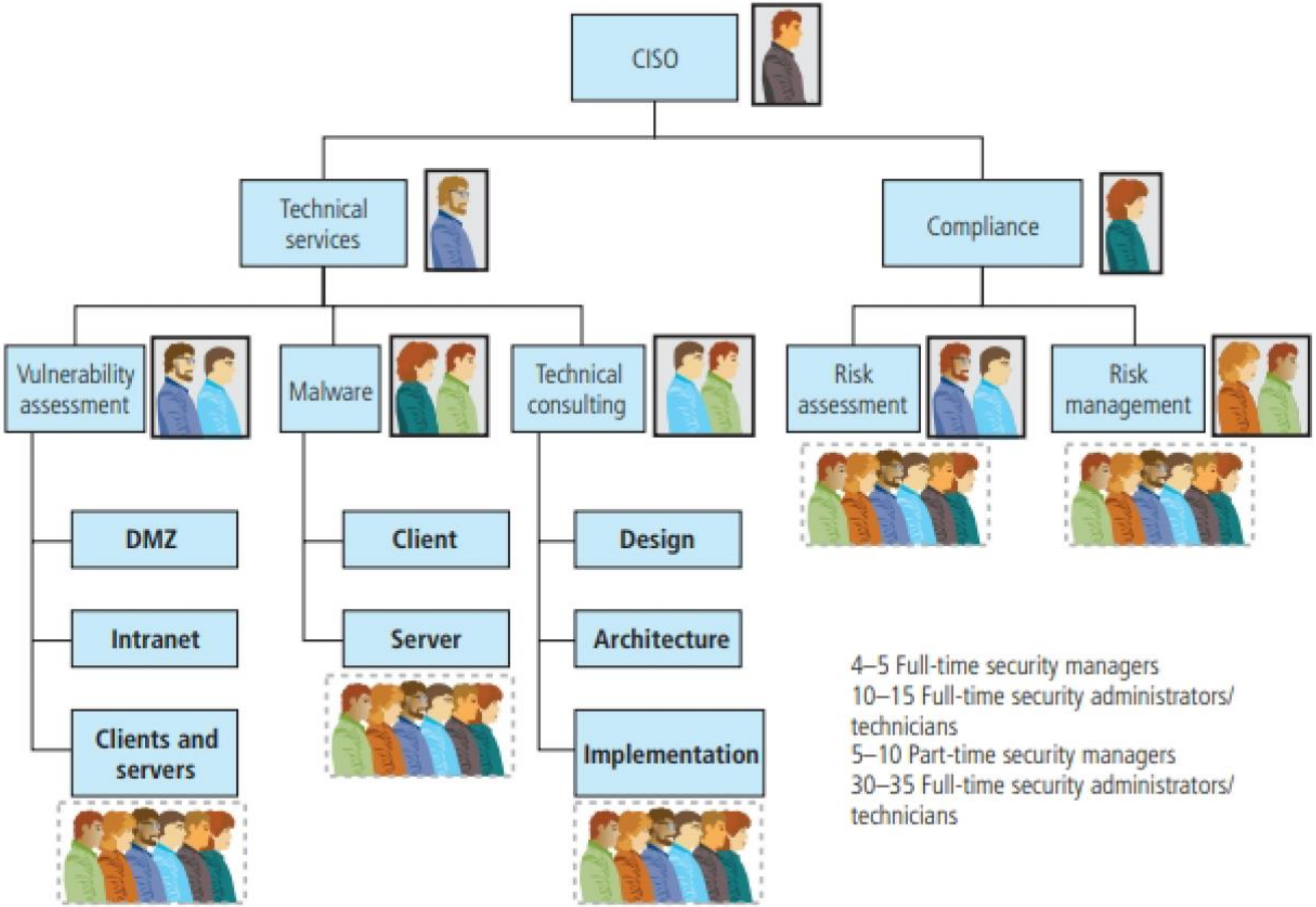
Very large organizations

- More than 10,000 computers

- Security budgets often grow faster than IT budgets

- Even with a large budgets, the average amount spent on security per user is still smaller than any other type of organization
  - ➢ Small organizations spend more than $5,000 per user on security; very large organizations spend about 1/18th of that, roughly $300 per user

Example: InfoSec Staffing in a Very Large Organization



4–5 Full-time security managers
10–15 Full-time security administrators/ technicians
5–10 Part-time security managers
30–35 Full-time security administrators/ technicians

Large organizations

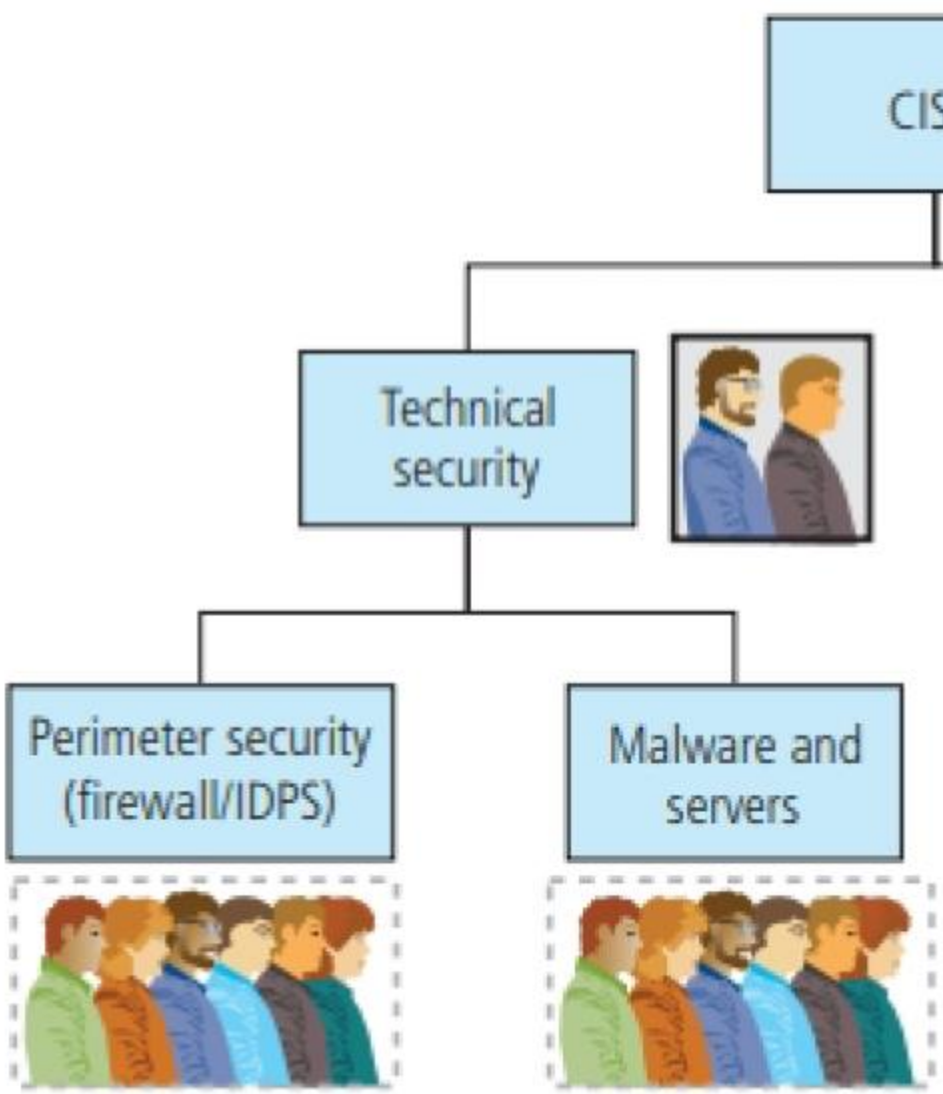
- 1,000 to 10,000 computers

- Security approach has often matured, integrating planning and policy into the organization’s culture

- Do not always put large amounts of resources into security
  - Considering the vast numbers of computers and users often involved

- They tend to spend proportionally less on security

Example: InfoSec Staffing in a Large Organization

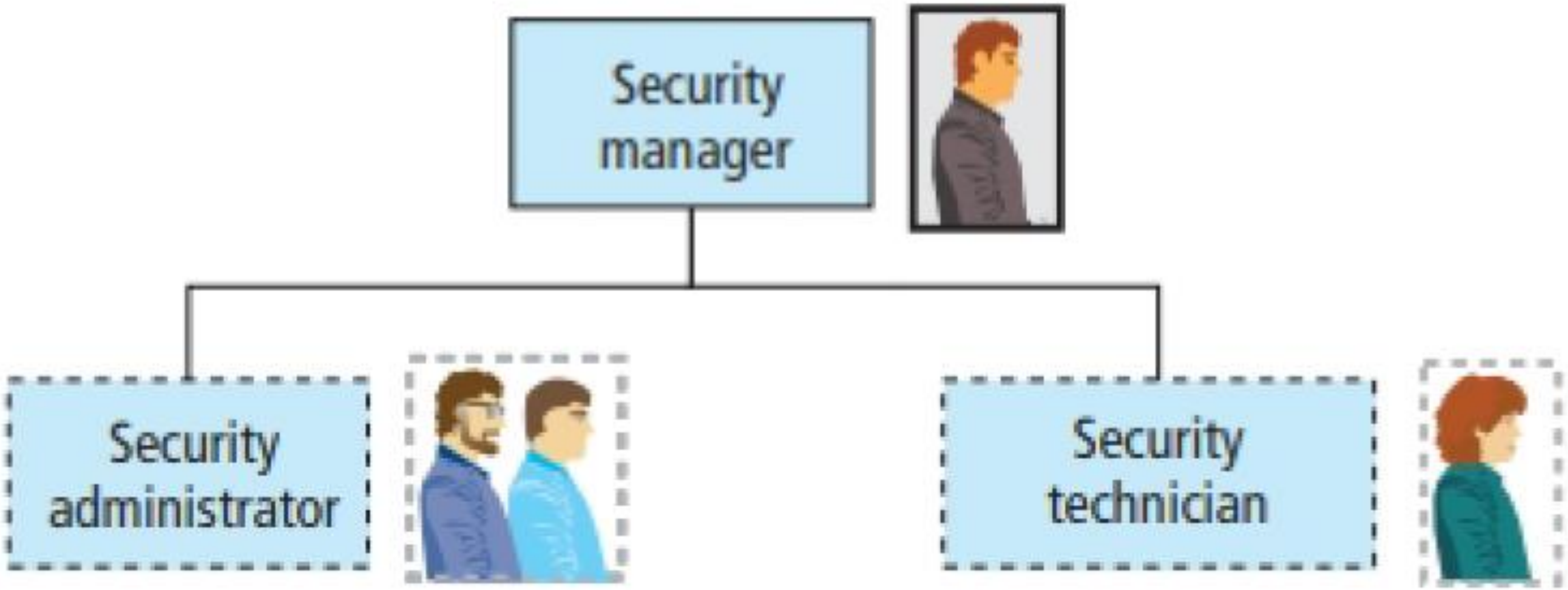

CISO
Technical security
Risk management and policy
Perimeter security (firewall/IDPS)
Malware and servers

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

Medium-sized organizations

- Have between 100 and 1000 computers
- Have a smaller total budget
- Have same sized security staff as the small organization, but a larger need
- Must rely on help from IT staff for plans and practices
- Ability to set policy, handle incidents, and effectively allocate resources is worse than any other size
- May be large enough to implement a multi-tiered approach to security
- Tend to ignore some security functions

Example: InfoSec Staffing in a Medium-Size Organization



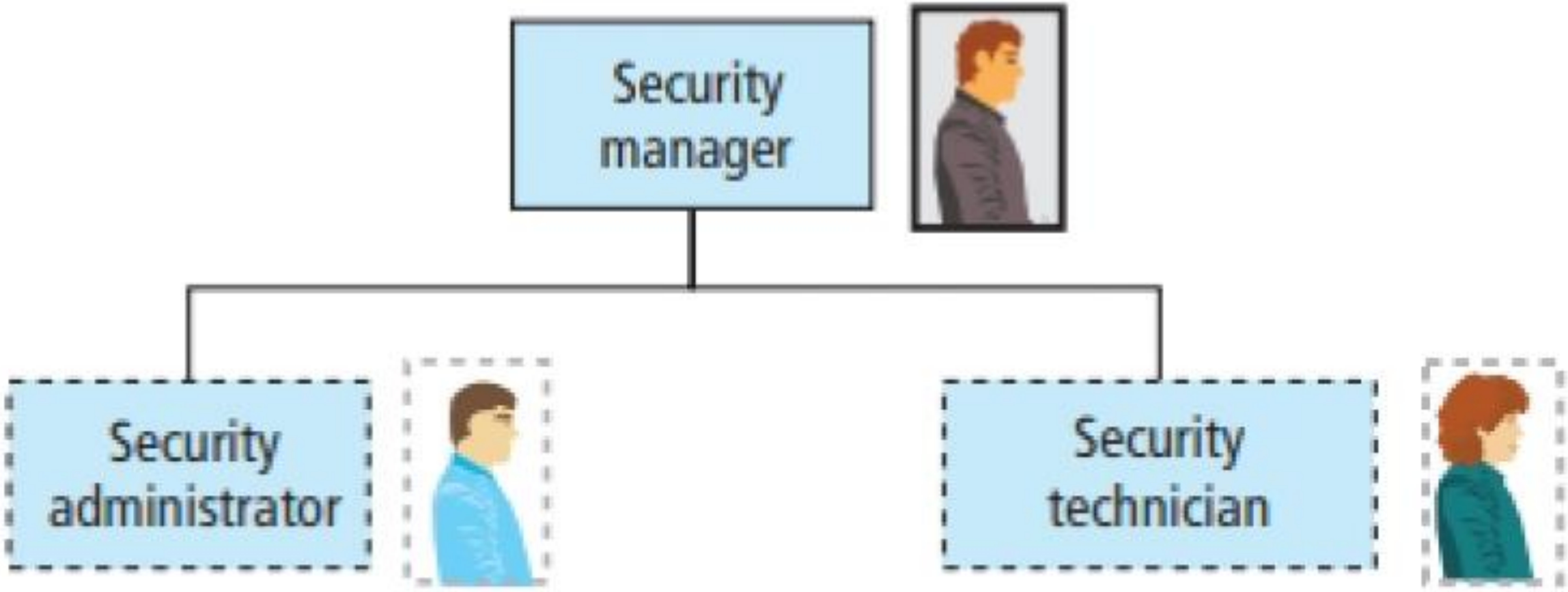
1 Full-time manager and partial-support staff members

Security in Small Organizations

Small organizations

- Have between 10 and 100 computers
- Have a simple, centralized IT organizational model
- Spend disproportionately more on security
- Information security is often the responsibility of a single security administrator
- Have little in the way of formal policy, planning, or security measures

Example: InfoSec Staffing in a Smaller Organization



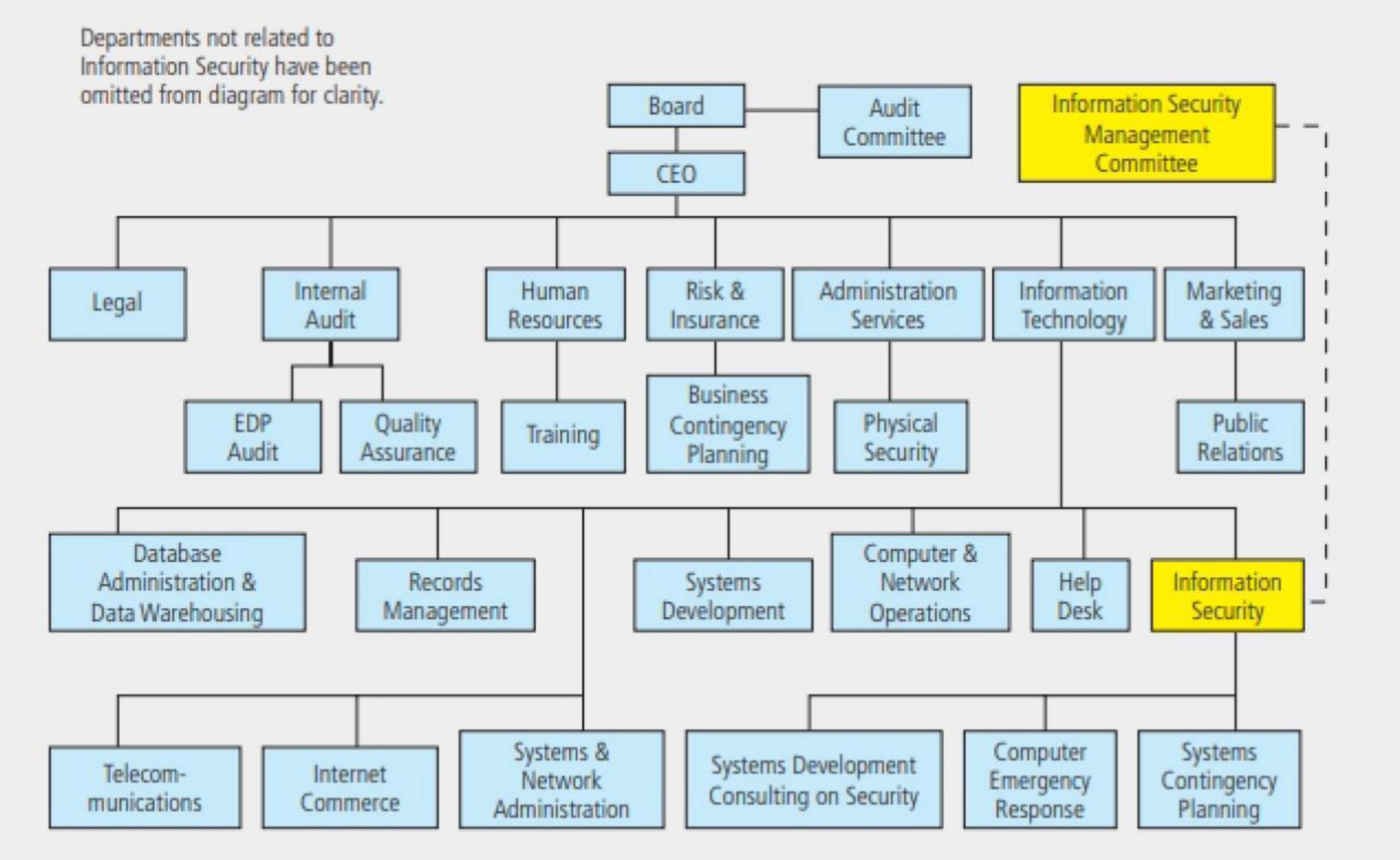
1 Full-time/part-time manager and part-time support staff members

Placing Information Security Within An Organization

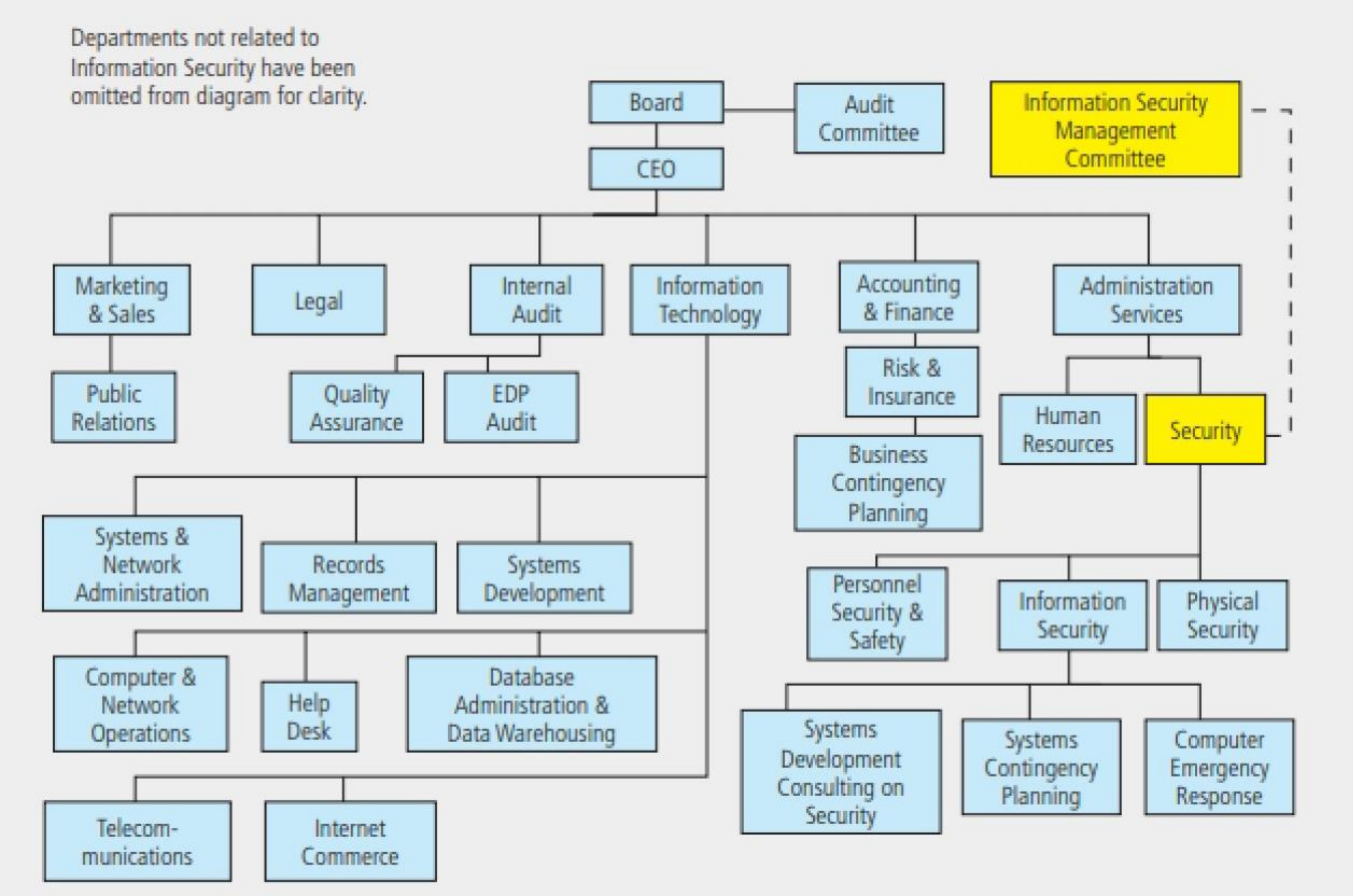
- Large organizations: InfoSec is often located within the IT department, headed by the CISO who reports directly to the CIO
- InfoSec program vs. the goals/objectives of IT dep. as a whole.
- The goals and objectives of the CIO and the CISO may come in conflict
  - ➢ The current movement to separate InfoSec from the IT division
  - ➢ The challenge is to design a reporting structure for the InfoSec program that balances the needs of each of the communities of interest

- Many ways to position the InfoSec program within an organization.
- In “Information Security Roles and Responsibilities Made Easy,” Wood compiled many of the best industry practices on InfoSec program.

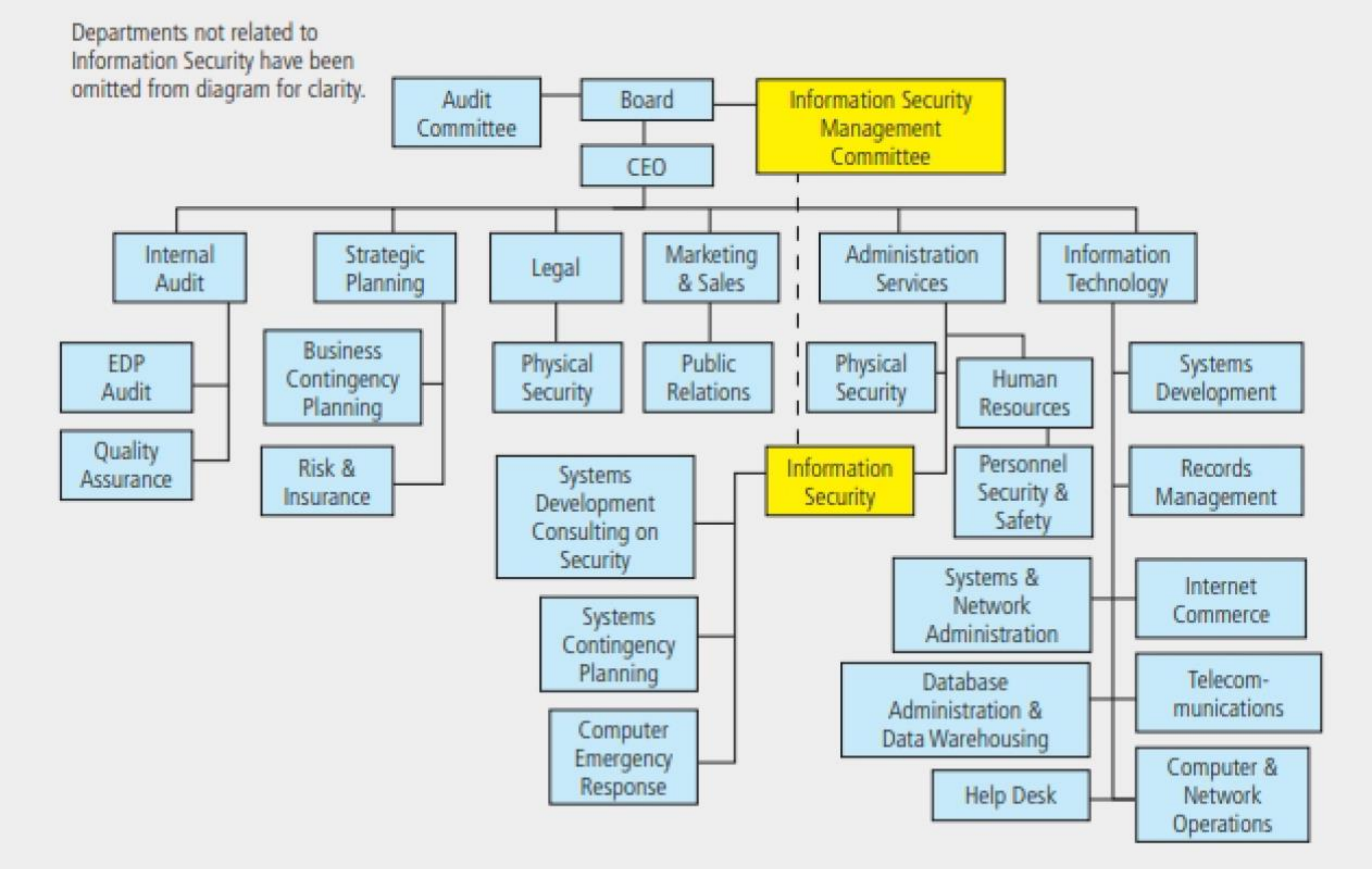
Option 1: InfoSec Reporting to IT Department


Departments not related to Information Security have been omitted from diagram for clarity.
Board
Audit Committee
Information Security Management Committee
CEO
Legal
Internal Audit
Human Resources
Risk & Insurance
Administration Services
Information Technology
Marketing & Sales
EDP Audit
Quality Assurance
Training
Business Contingency Planning
Physical Security
Public Relations
Database Administration & Data Warehousing
Records Management
Systems Development
Computer & Network Operations
Help Desk
Information Security
Telecom-munications
Internet Commerce
Systems & Network Administration
Systems Development Consulting on Security
Computer Emergency Response
Systems Contingency Planning

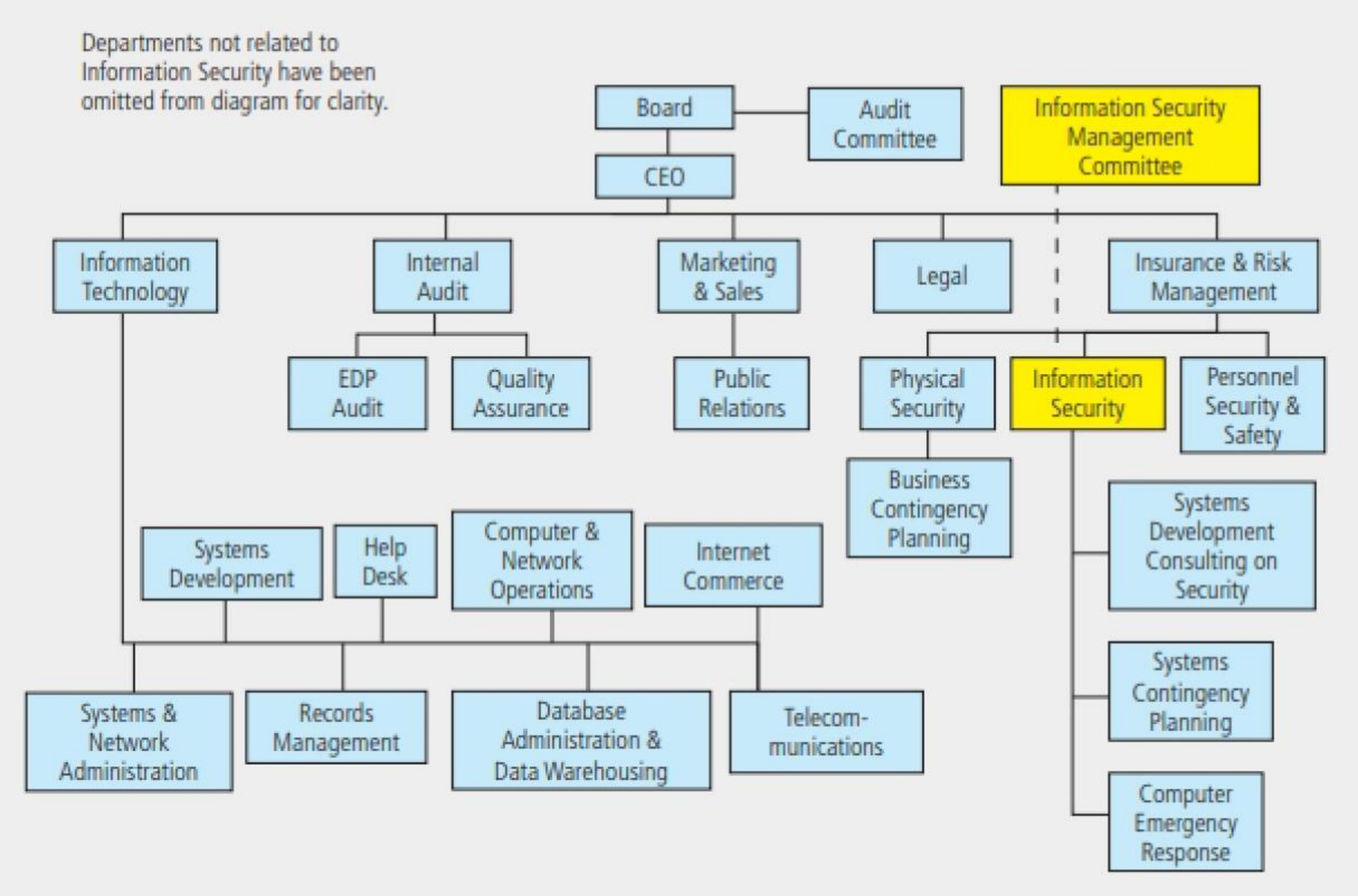
Option 2: InfoSec Reporting to Security Department


Departments not related to Information Security have been omitted from diagram for clarity.
Board
Audit Committee
Information Security Management Committee
CEO
Marketing & Sales
Legal
Internal Audit
Information Technology
Accounting & Finance
Administration Services
Public Relations
Quality Assurance
EDP Audit
Risk & Insurance
Human Resources
Security
Business Contingency Planning
Systems & Network Administration
Records Management
Systems Development
Personnel Security & Safety
Information Security
Physical Security
Computer & Network Operations
Help Desk
Database Administration & Data Warehousing
Systems Development Consulting on Security
Systems Contingency Planning
Computer Emergency Response
Telecom-munications
Internet Commerce

Option 3: InfoSec Reporting to Administrative Services Department

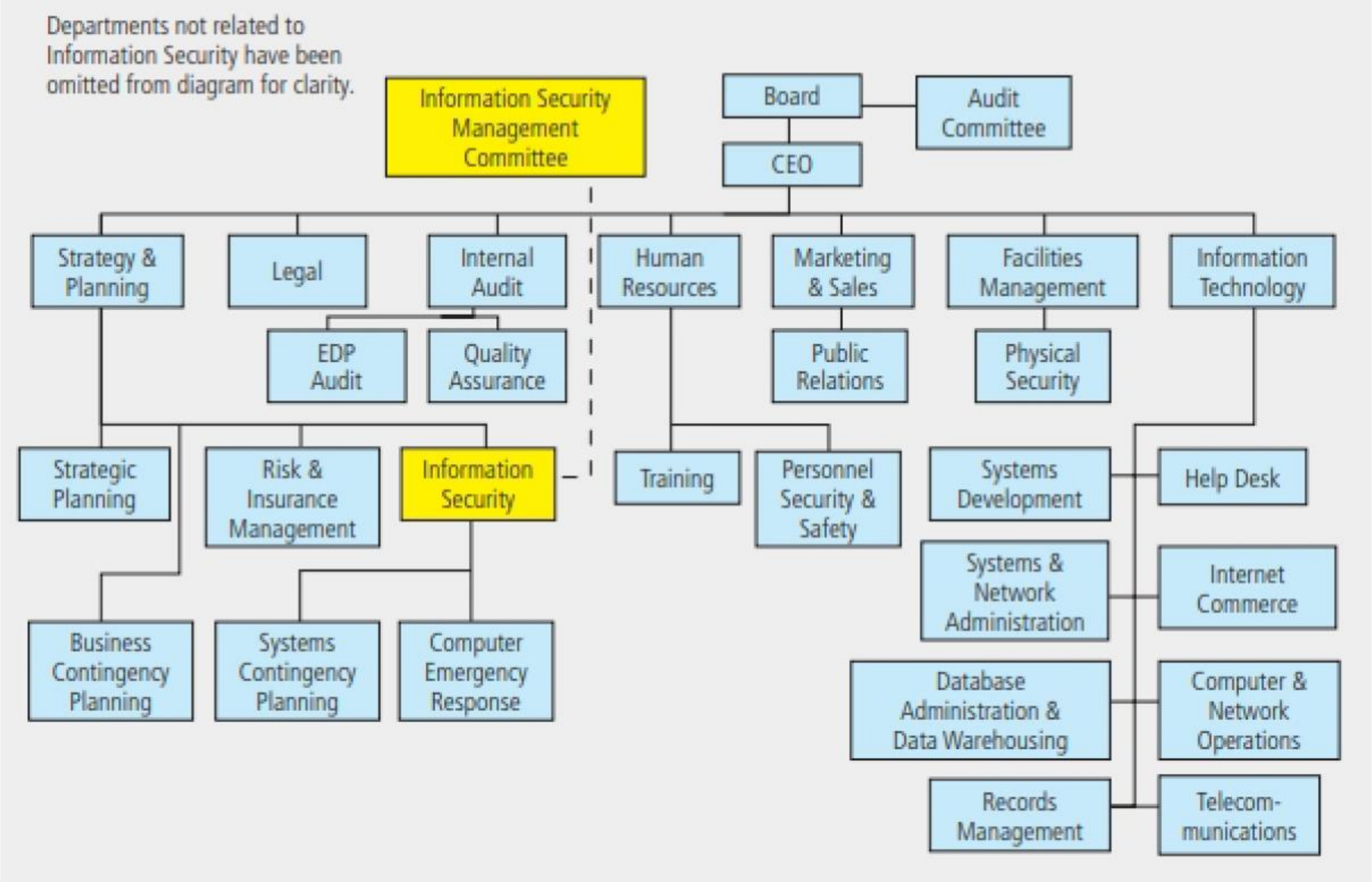

Departments not related to Information Security have been omitted from diagram for clarity.
Audit Committee
Board
Information Security Management Committee
CEO
Internal Audit
Strategic Planning
Legal
Marketing & Sales
Administration Services
Information Technology
EDP Audit
Quality Assurance
Business Contingency Planning
Risk & Insurance
Physical Security
Public Relations
Physical Security
Human Resources
Systems Development
Information Security
Personnel Security & Safety
Records Management
Systems Development Consulting on Security
Systems Contingency Planning
Computer Emergency Response
Systems & Network Administration
Internet Commerce
Database Administration & Data Warehousing
Telecom-munications
Help Desk
Computer & Network Operations

Option 4: InfoSec Reporting to Insurance and Risk Management Department


Departments not related to Information Security have been omitted from diagram for clarity.

Board
Audit Committee
Information Security Management Committee
CEO
Information Technology
Internal Audit
Marketing & Sales
Legal
Insurance & Risk Management
EDP Audit
Quality Assurance
Public Relations
Physical Security
Information Security
Personnel Security & Safety
Business Contingency Planning
Systems Development Consulting on Security
Systems Contingency Planning
Computer Emergency Response
Systems Development
Help Desk
Computer & Network Operations
Internet Commerce
Systems & Network Administration
Records Management
Database Administration & Data Warehousing
Telecom-munications

Option 5: InfoSec Reporting to Strategy and Planning Department


Departments not related to Information Security have been omitted from diagram for clarity.
Information Security Management Committee
Board
Audit Committee
CEO
Strategy & Planning
Legal
Internal Audit
Human Resources
Marketing & Sales
Facilities Management
Information Technology
EDP Audit
Quality Assurance
Public Relations
Physical Security
Strategic Planning
Risk & Insurance Management
Information Security
Training
Personnel Security & Safety
Systems Development
Help Desk
Systems & Network Administration
Internet Commerce
Database Administration & Data Warehousing
Computer & Network Operations
Records Management
Telecom-munications
Business Contingency Planning
Systems Contingency Planning
Computer Emergency Response

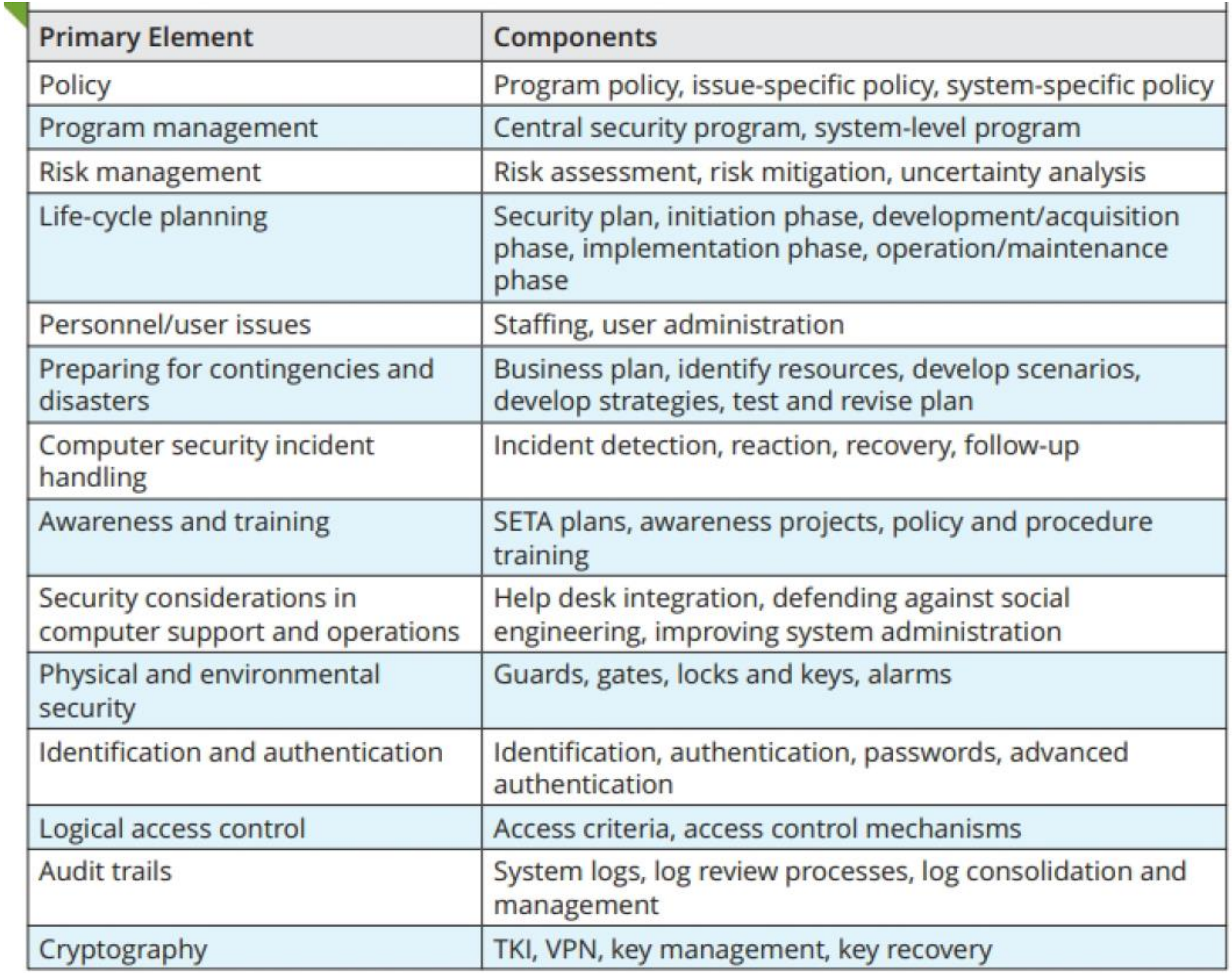
Placing Information Security Within an Organization (cont’d.)

- **Other options**
  - Option 6: Legal
  - Option 7: Internal audit (not advised)
  - Option 8: Help desk (not advised)
  - Option 9: Accounting and finance through IT (not advised)
  - Option 10: Human resources (not advised)
  - Option 11: Facilities management
  - Option 12: Operations

Components of the Security Program

- Organization’s information security needs are unique to the culture, size, and budget of the organization.
- Determining the level at which the InfoSec program operates depends on the organization’s strategic plan -- in particular, the plan’s vision and mission statements. The CIO and CISO should use these two documents to formulate the mission statement for the InfoSec program

- **NIST’s documents**
  - ➢ SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems
  - ➢ SP 800-12, An Introduction to Computer Security: The NIST Handbook



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 disasters	Business plan, identify resources, develop scenarios, develop strategies, test and revise plan
Computer security incident handling	Incident detection, reaction, recovery, follow-up
Awareness and training	SETA plans, awareness projects, policy and procedure training
Security considerations in computer support and operations	Help desk integration, defending against social engineering, improving system administration
Physical and environmental security	Guards, gates, locks and keys, alarms
Identification and authentication	Identification, authentication, passwords, advanced authentication
Logical access control	Access criteria, access control mechanisms
Audit trails	System logs, log review processes, log consolidation and management
Cryptography	TKI, VPN, key management, key recovery

Source: NIST.

Information Security Roles and Titles

Types of InfoSec positions (Schwartz, Erwin, Weafer, and Briney)

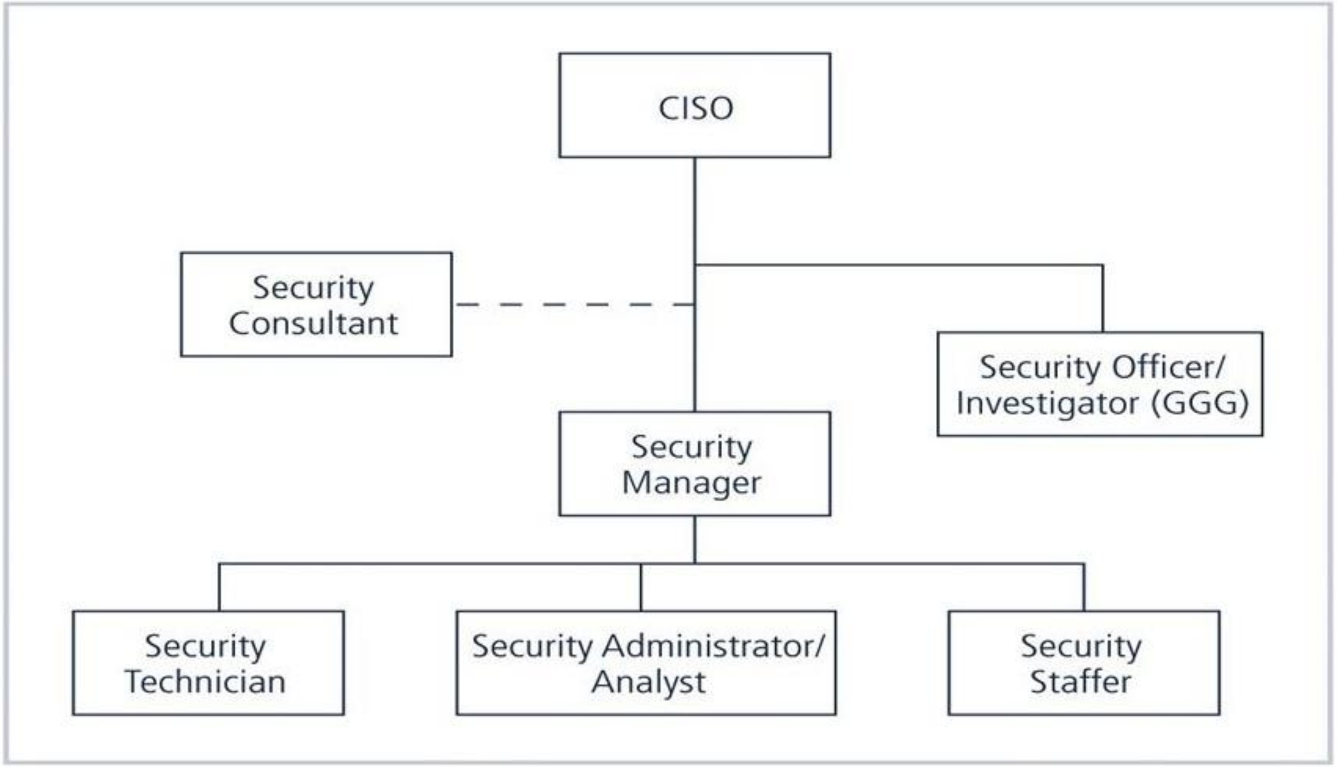
- **Those that define**
  - ➢ Provide the policies, guidelines, and standards
  - ➢ Do the consulting and the risk assessment
  - ➢ Develop the product and technical architectures
  - ➢ Senior people with a lot of broad knowledge, but often not a lot of depth

- **Those that build**
  - ➢ The real “techies” who create and install security solutions

- **Those that administer**
  - ➢ Operate and administer the security tools and the security monitoring function
  - ➢ Continuously improve the processes

A typical organization has a number of individuals with InfoSec responsibilities. Most of the job functions fit into one of the following:

- CISO
- Security managers
- Security admin/analysts
- Security technicians
- Security staffers/watchstanders
- Security consultants
- Security officers/investigators
- Help desk personnel



Implementing SETA Programs

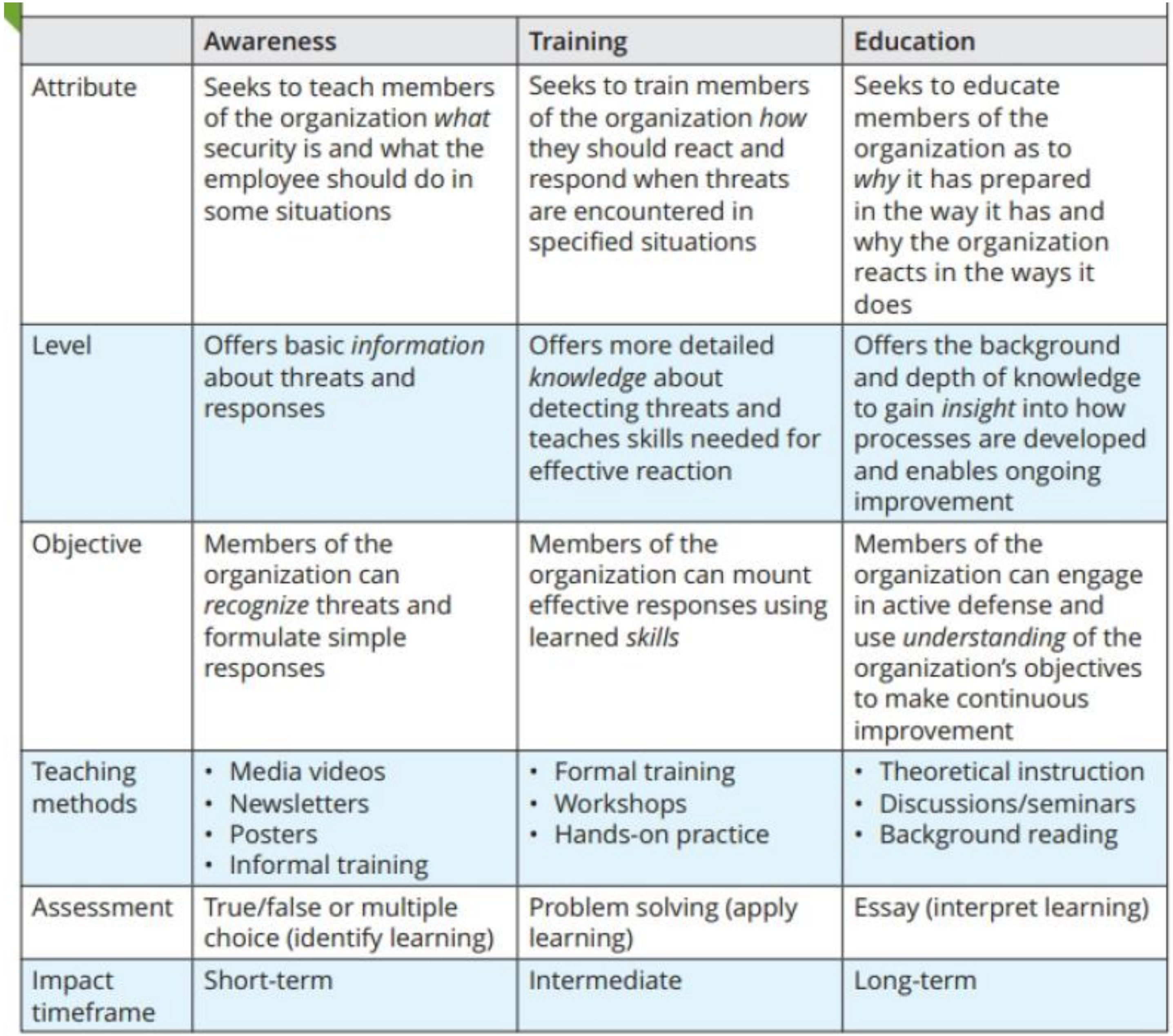
SETA | SECURITY EDUCATION TRAINING AWARENESS

- **SETA programs**
  - Responsibility of the CISO
  - Designed to reduce accidental security breaches
  - Three elements: security education, security training, security awareness

- **SETA programs offer three major benefits:**
  - Improve employee behavior
  - Inform members where to report
  - Enable the organization to hold employees accountable for their actions

The purpose of SETA is to enhance security in three ways:

1. By building in-depth knowledge, to design, implement, or operate security programs for organizations and systems
2. By developing skills and knowledge so that computer users can perform their jobs while using IT systems more securely
3. By improving awareness of the need to protect system resources



	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* it has prepared in the way it has and why the organization reacts in the ways 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 organization's objectives to make continuous improvement
Teaching methods	• Media videos • Newsletters • Posters • Informal training	• Formal training • Workshops • Hands-on practice	• Theoretical instruction • Discussions/seminars • Background reading
Assessment	True/false or multiple choice (identify learning)	Problem solving (apply learning)	Essay (interpret learning)
Impact timeframe	Short-term	Intermediate	Long-term

Source: NIST SP 800-12.

Security Education

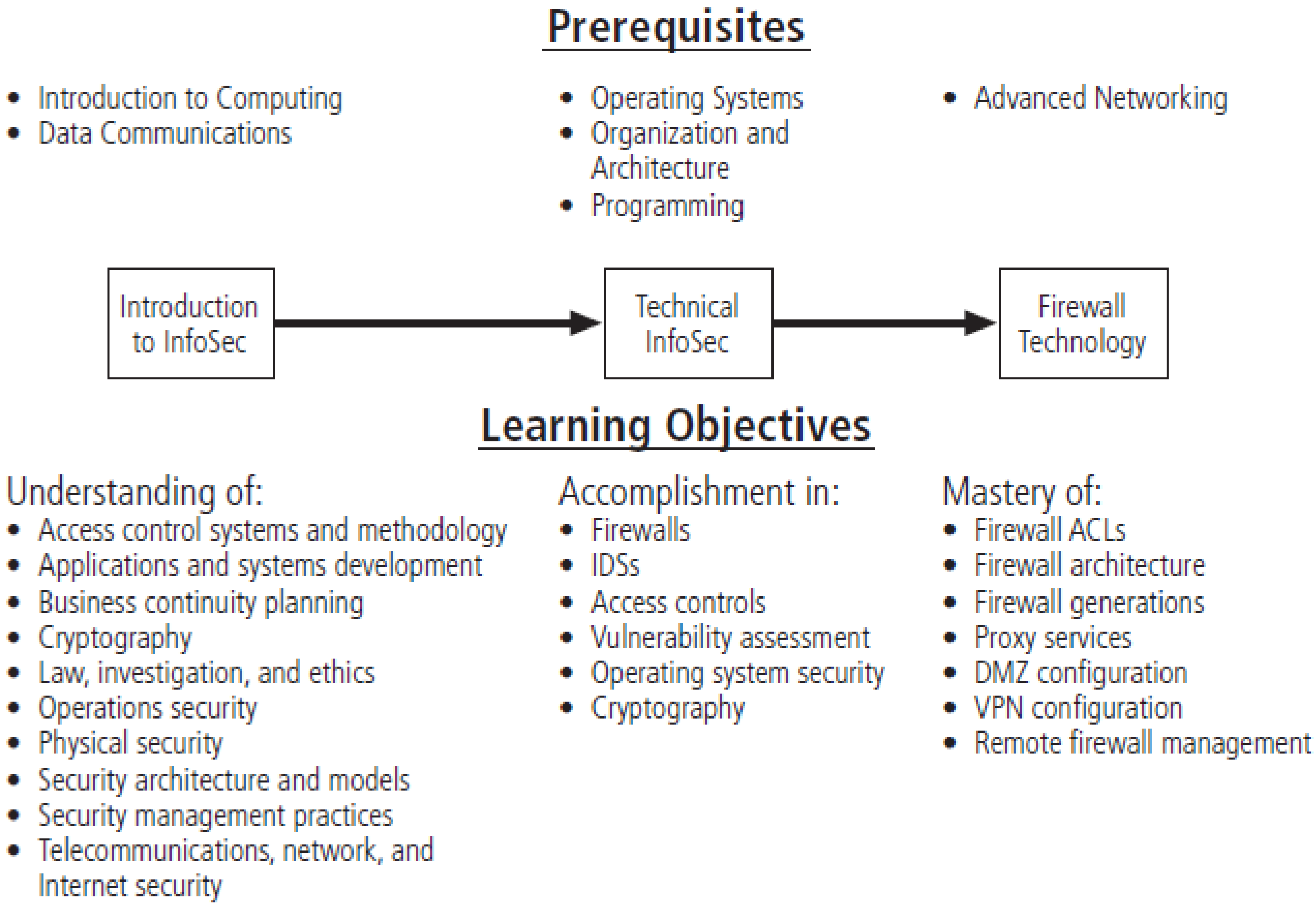
- InfoSec employees may be encouraged to seek a formal education
  - ➢ If not prepared by their background or experience

- InfoSec education 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
  - ➢ General knowledge that all business professionals must understand

- Many colleges and universities provide formal coursework in InfoSec
  - ➢ Unfortunately, most security-related degrees are computer science or information systems degrees that include a few courses in security

- Certifications for InfoSec professionals
  - ➢ CISSP, CISM, GISO, GIAC, Security+

Security Education (cont'd.)



Prerequisites

- Introduction to Computing
- Data Communications

- Operating Systems
- Organization and Architecture
- Programming

- Advanced Networking

Learning Objectives

Understanding of:
- Access control systems and methodology
- Applications and systems development
- Business continuity planning
- Cryptography
- Law, investigation, and ethics
- Operations security
- Physical security
- Security architecture and models
- Security management practices
- Telecommunications, network, and Internet security

Accomplishment in:
- Firewalls
- IDSs
- Access controls
- Vulnerability assessment
- Operating system security
- Cryptography

Mastery of:
- Firewall ACLs
- Firewall architecture
- Firewall generations
- Proxy services
- DMZ configuration
- VPN configuration
- Remote firewall management

Security Training

- Involves providing detailed information and hands-on instruction
    - ➢ To develop user skills to perform their duties securely
- Management can either develop customized training or outsource
- Customizing training for users
    - ➢ By functional background: General user; Managerial user; Technical user
    - ➢ By skill level: Novice; Intermediate; Advanced

Trainings by Functional Background

- **Training for general users**
  - ➢ Training on policies: users can ask questions and receive specific guidance; organization can collect the required letters of compliance
  - ➢ Training on technical details

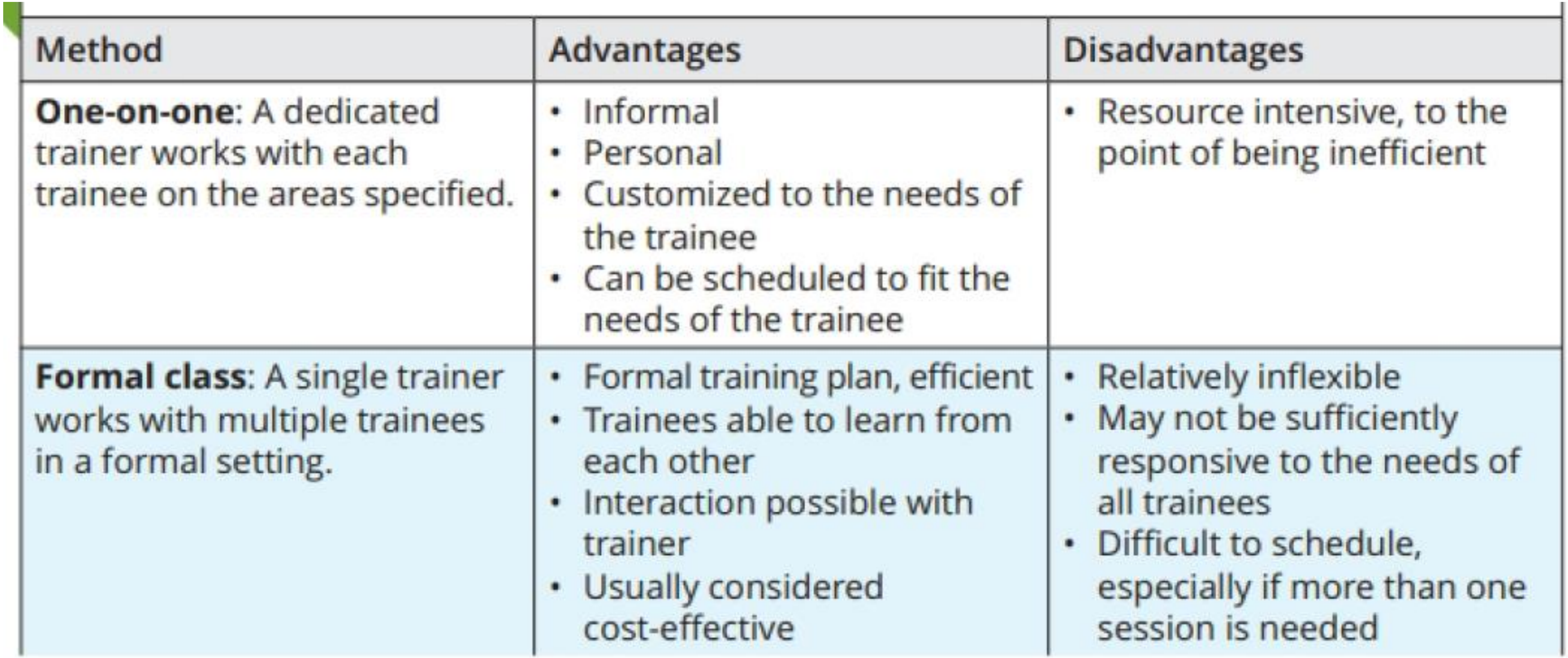
- **Training for managerial users**
  - ➢ Managers typically expect a more personal form of training

- **Training for technical users**
  - ➢ More detailed than general users or managerial training
  - ➢ May require consultants or outside training organizations
  - ➢ Methods for selecting and developing advanced technical training: by job category, by job function and by technology product

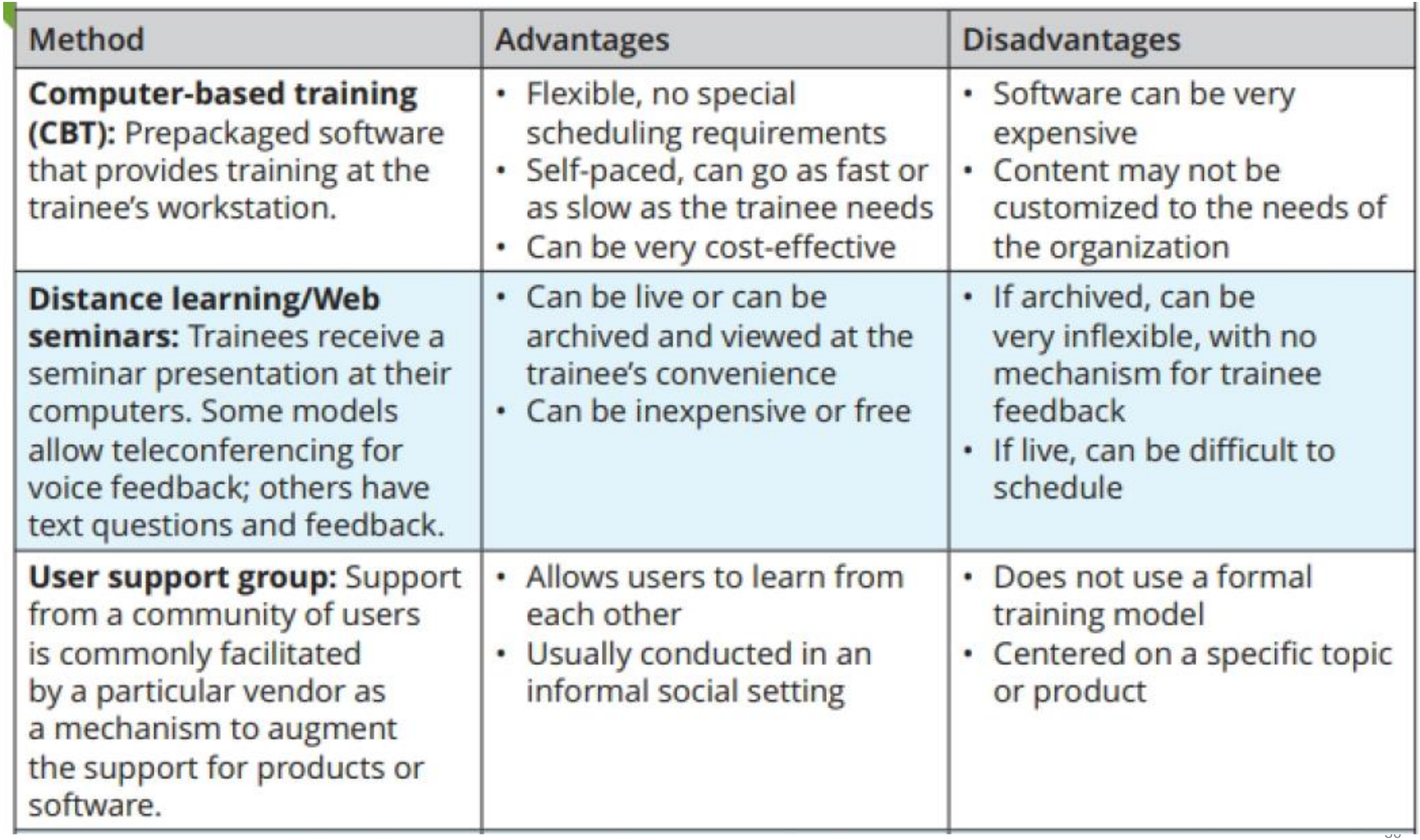
Training Delivery Methods

- Selection of the training delivery method is not always based on the best outcome for the trainee
  - ➢ Often overridden by budget, scheduling, and needs of the organization

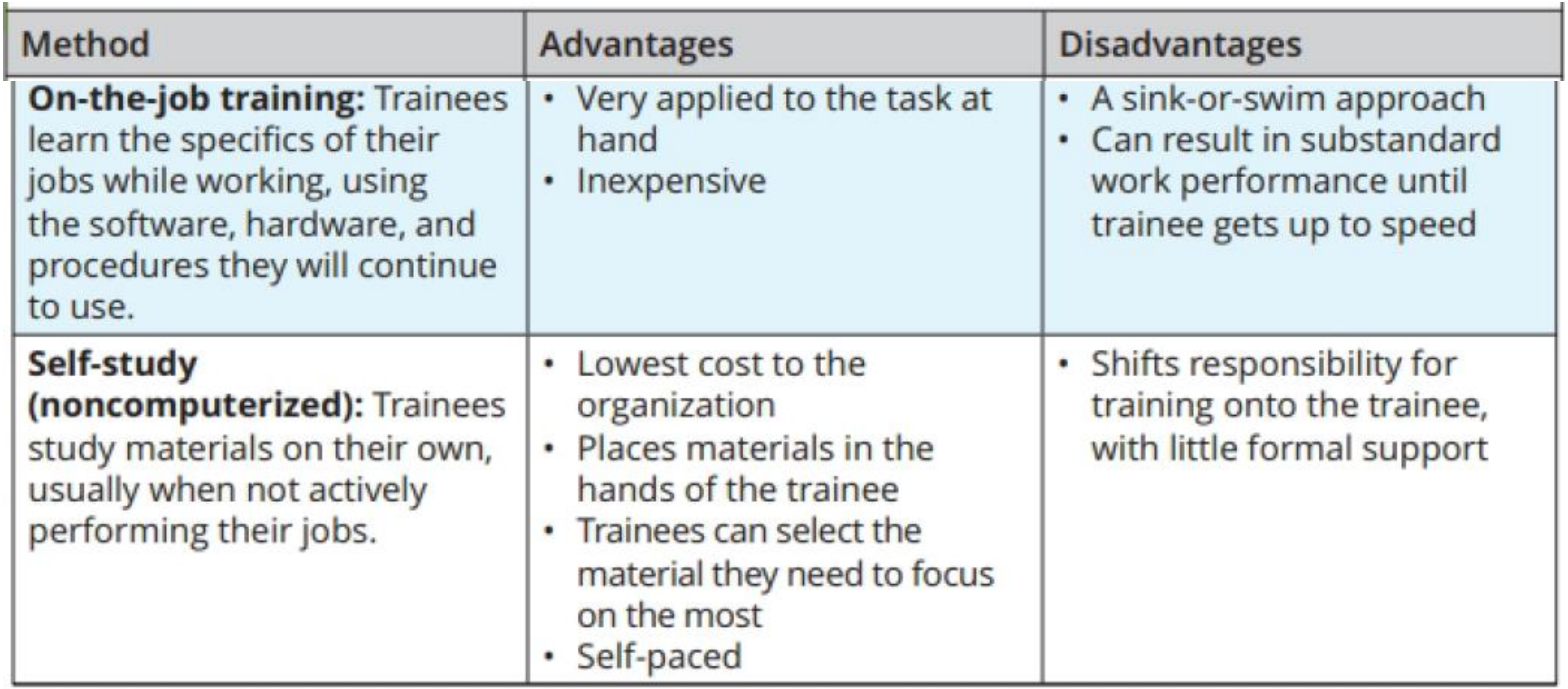
- **Types of delivery methods**
  - ➢ One-on-one
  - ➢ Formal class
  - ➢ Computer-based training (CBT)
  - ➢ Distance learning/web seminars
  - ➢ User support group
  - ➢ On-the-job training
  - ➢ Self-study (non-computerized)



Method	Advantages	Disadvantages
One-on-one: A dedicated trainer works with each trainee on the areas specified.	• Informal • Personal • Customized to the needs of the trainee • Can be scheduled to fit the needs of the trainee	• Resource intensive, to the point of being inefficient
Formal class: A single trainer works with multiple trainees in a formal setting.	• Formal training plan, efficient • Trainees able to learn from each other • Interaction possible with trainer • Usually considered cost-effective	• Relatively inflexible • May not be sufficiently responsive to the needs of all trainees • Difficult to schedule, especially if more than one session is needed



Method	Advantages	Disadvantages
Computer-based training (CBT): Prepackaged software that provides training at the trainee's workstation.	• Flexible, no special scheduling requirements • Self-paced, can go as fast or as slow as the trainee needs • Can be very cost-effective	• Software can be very expensive • 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 • Can be inexpensive or free	• If archived, can be very inflexible, with no mechanism for trainee feedback • If live, can be difficult to schedule
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 • Usually conducted in an informal social setting	• Does not use a formal training model • Centered on a specific topic or product



Method	Advantages	Disadvantages
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 • Inexpensive	• A sink-or-swim approach • 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 • Places materials in the hands of the trainee • Trainees can select the material they need to focus on the most • Self-paced	• Shifts responsibility for training onto the trainee, with little formal support

Selecting the Training Staff

To provide training, an organization can

- Use a local training program
- Use a continuing education department
- Use another external training agency
- Hire a professional trainer, a consultant, or someone from an accredited institution to conduct on-site training
- Organize and conduct training in-house using organization's own employees

Implementing Training

Seven-step methodology

1	Identify program scope/goals/objectives
2	Identify training staff
3	Identify target audiences (*)
4	Motivate management and employees
5	Administer the program
6	Maintain the program
7	Evaluate the program

(*) Employees can be divided into groups in the following ways:

1. By level of awareness
2. By general job task or function
3. By specific job category
4. By level of computer knowledge
5. By types of technology or systems used

Security Awareness

- Security awareness program: One of the least frequently implemented, but most effective security methods

- As noted in NIST SP 800-12, 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

Security Awareness (cont'd.)

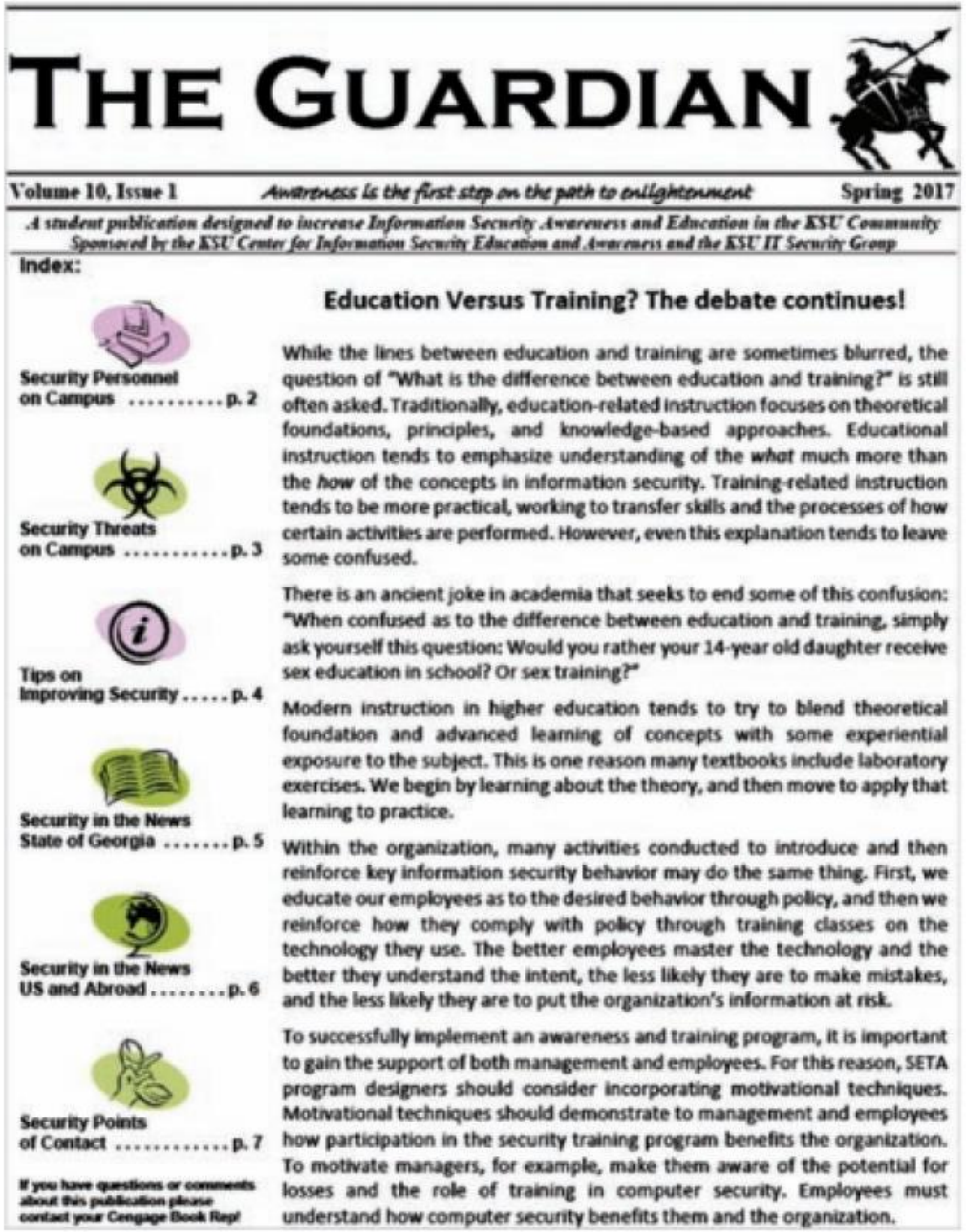
When developing an awareness program, be sure to do the following:

1. Focus on people
2. Refrain from using technical jargon
3. Use every available venue
4. Define learning objectives, state clearly, provide sufficient detail and coverage
5. Keep things light
6. Don't overload the users
7. Help users understand their roles in InfoSec
8. Take advantage of in-house communications media
9. Make the awareness program formal; plan and document all actions
10. Provide good information early, rather than perfect information late

Security Awareness Components

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
- Website



THE GUARDIAN

Volume 10, Issue 1 *Awareness is the first step on the path to enlightenment* Spring 2017

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:

If you have questions or comments about this publication please contact your Cengage Book Rep!

Education Versus Training? The debate continues!

While the lines between education and training are sometimes blurred, the question of "What is the difference between education and training?" is still often asked. Traditionally, education-related instruction focuses on theoretical foundations, principles, and knowledge-based approaches. Educational instruction tends to emphasize understanding of the *what* much more than the *how* of the concepts in information security. Training-related instruction tends to be more practical, working to transfer skills and the processes of how certain activities are performed. However, even this explanation tends to leave some confused.

There is an ancient joke in academia that seeks to end some of this confusion: "When confused as to the difference between education and training, simply ask yourself this question: Would you rather your 14-year old daughter receive sex education in school? Or sex training?"

Modern instruction in higher education tends to try to blend theoretical foundation and advanced learning of concepts with some experiential exposure to the subject. This is one reason many textbooks include laboratory exercises. We begin by learning about the theory, and then move to apply that learning to practice.

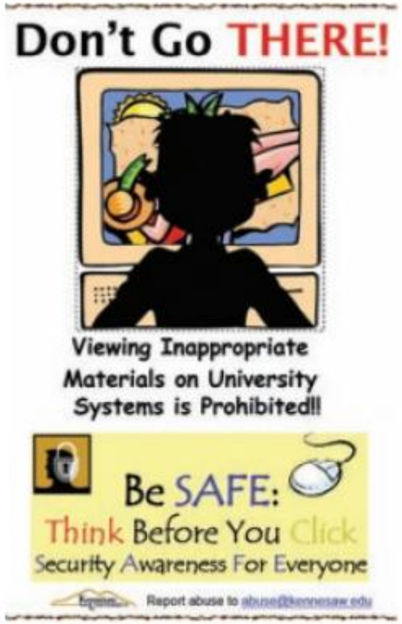
Within the organization, many activities conducted to introduce and then reinforce key information security behavior may do the same thing. First, we educate our employees as to the desired behavior through policy, and then we reinforce how they comply with policy through training classes on the technology they use. The better employees master the technology and the better they understand the intent, the less likely they are to make mistakes, and the less likely they are to put the organization's information at risk.

To successfully implement an awareness and training program, it is important to gain the support of both management and employees. For this reason, SETA program designers should consider incorporating motivational techniques. Motivational techniques should demonstrate to management and employees how participation in the security training program benefits the organization. To motivate managers, for example, make them aware of the potential for losses and the role of training in computer security. Employees must understand how computer security benefits them and the organization.

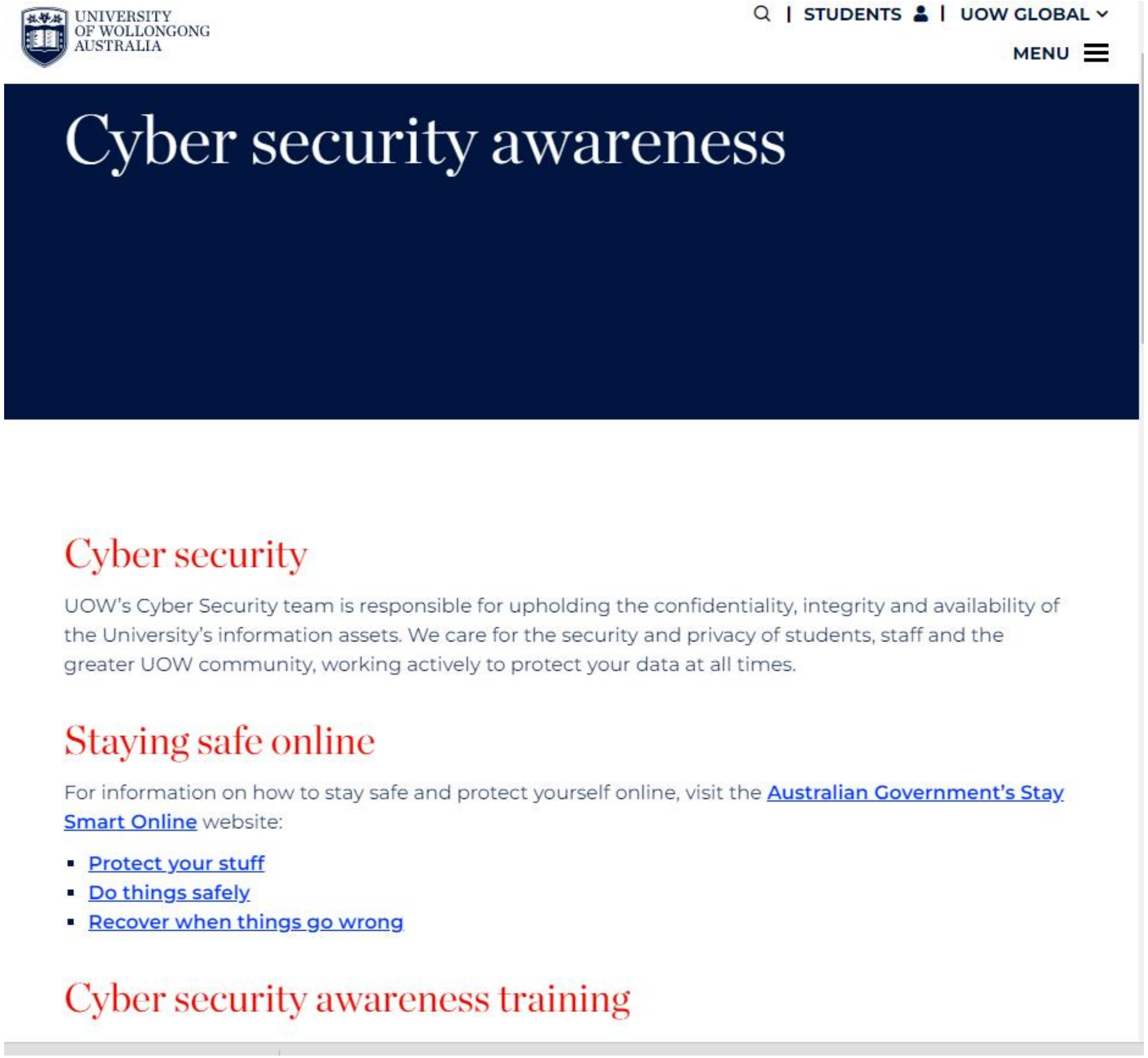
Introducing
Kennesaw State University's
new
Information Security Awareness Program!!
Be SAFE:
Think Before You Click
Security Awareness For Everyone
When you see these messages,
Think about information security.
Help us protect the information and systems vital to the University!
Report abuse to abuse@kennesaw.edu

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 …
hard drive not found
insert system disk
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

SECURITY
Southeast Collegiate Cyber Defense Competition
Kennesaw State University
Center for Information Security Education
InfoSecCD
CENGAGE Learning
21ST ANNUAL COMPUTING CONFERENCE
KPMG
radware
SECUREWORLD
cyberspaceskills.com
INSCOM Cyber Brigade
IBM Security
cloud



Cyber security awareness

Cyber security

UOW's Cyber Security team is responsible for upholding the confidentiality, integrity and availability of the University's information assets. We care for the security and privacy of students, staff and the greater UOW community, working actively to protect your data at all times.

Staying safe online

For information on how to stay safe and protect yourself online, visit the Australian Government's Stay Smart Online website:

- Protect your stuff
- Do things safely
- Recover when things go wrong

Cyber security awareness training