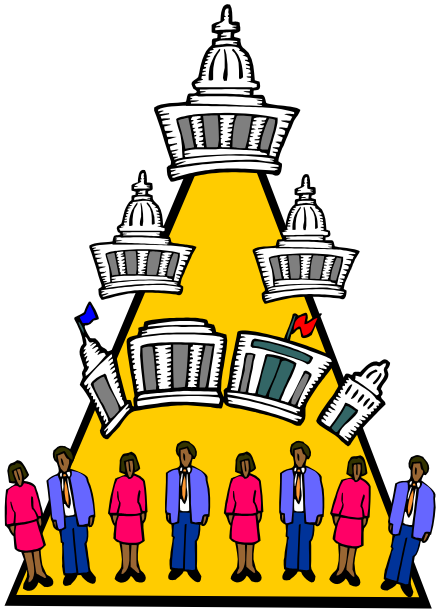
Securing the Organization and Business continuity

Securing Organizations

Organizations

Managers



Employees
(End users)

Mangers are often faced with resource constraints
→ cumbersome practices
→ non-compliance by employees

Developing the Security Program

Introduction

- Some organizations use security programs to describe the entire set of personnel, plans, policies, and initiatives related to information security
- Information security program: used here to describe the structure and organization of the effort used to secure information assets of organization

Organizing for Security

- Some variables that determine how to structure an information security program are:
  - Organizational culture
  - Size
  - Security personnel budget
  - Security capital budget

as organizations get larger in size, their security departments more often do not keep up with the demands of increasingly complex organizational infrastructures. Security spending per user and per machine declines exponentially as organizations grow, leaving most handcuffed when it comes to implementing effective security procedures.

Security in Large Organizations

- Information security departments in large organizations tend to form and re-form internal groups to meet long-term challenges even as they handle day-to-day security operations
- Functions are likely to be split into groups
- In contrast, smaller organizations typically create fewer groups, perhaps only having one general group representing the communities of interest

Very Large Organizations More than 10,000 Computers

- Security budgets often grow faster than IT budgets
- Studies indicate that even with large budgets, average amount spent on security per user is still smaller than any other type of organization

  Where small orgs may spend more than $5,000 per user on security, very large organizations may spend about 1/18th of that, roughly $300 per user

Large Organizations With 1,000 to 10,000 computers

- At this size, approach to security has often matured, integrating planning and policy into organization's culture
- Unfortunately, large organization do not always put large amounts of resources into security considering vast numbers of computers and users often involved
- Tend to spend proportionally less on security

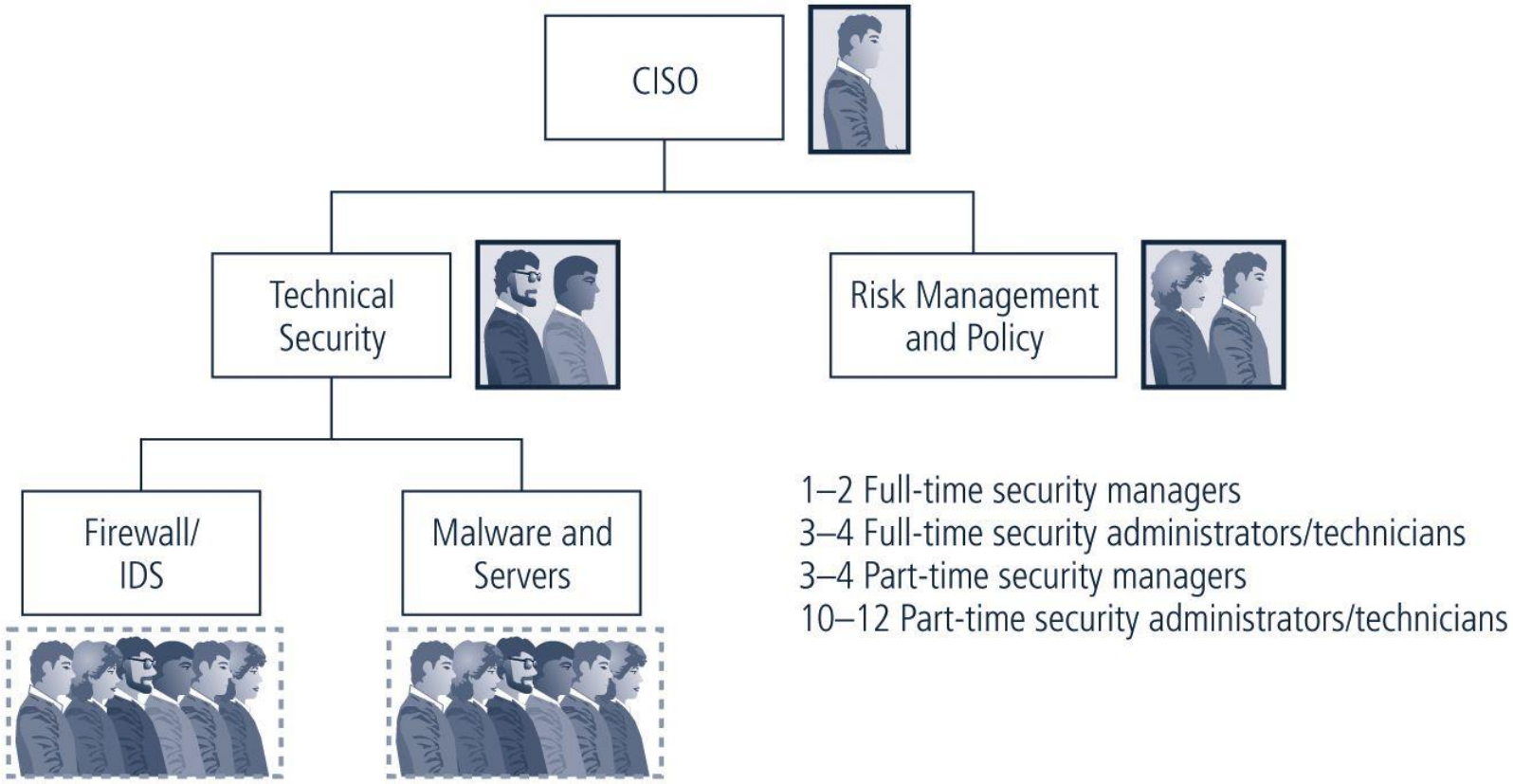
Security in Large Organizations

- One recommended approach is to separate functions into 4 areas:
  - Functions performed by non-technology business units outside of IT
  - Functions performed by IT groups outside of information security area
  - Functions performed within information security department as customer service
  - Functions performed within the information security department as compliance

Responsibilities in Large Organizations

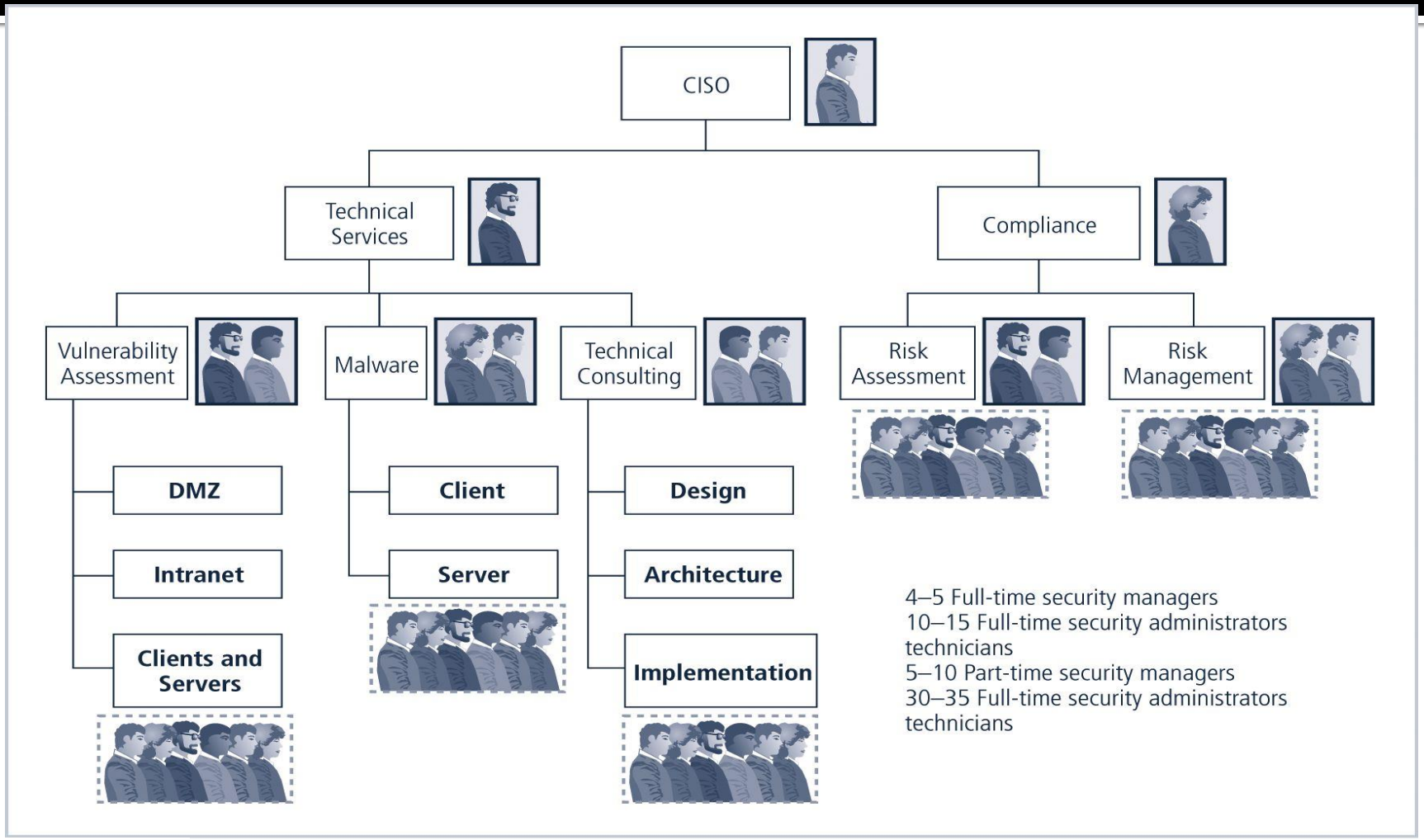
- It's CISO's responsibility to see that information security functions are adequately performed within the organization
- Deployment of full-time security personnel depends on a number of factors, including sensitivity of information to be protected, industry regulations and general profitability
- The more money a company can dedicate to its personnel budget, the more likely it is to maintain a large information security staff

Information Security Staffing in a Large Organization



Information Security Staffing in a Large Organization

InfoSec Staffing in a Very Large Organization



Information Security Staffing in a Very Large Organization

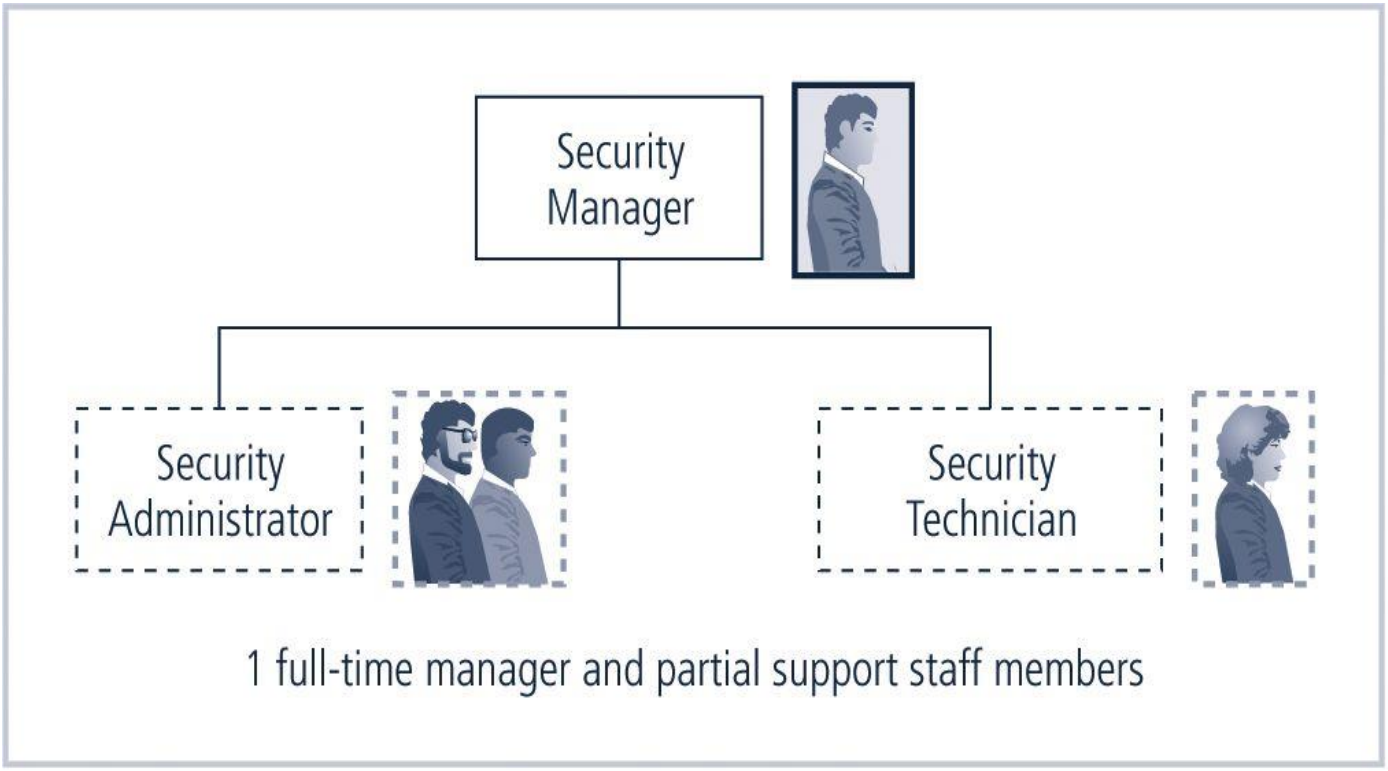
Security in Medium-Sized Organizations 100-1,000 Computers

- Have smaller total budget
- Have same sized security staff as small org, but larger need
- Must rely on help from IT staff for plans and practices
- Have challenge in setting policy, handling incidents in regular manner and effectively allocating resources

Security in Medium-Sized Organizations 100-1,000 Computers (Continued)

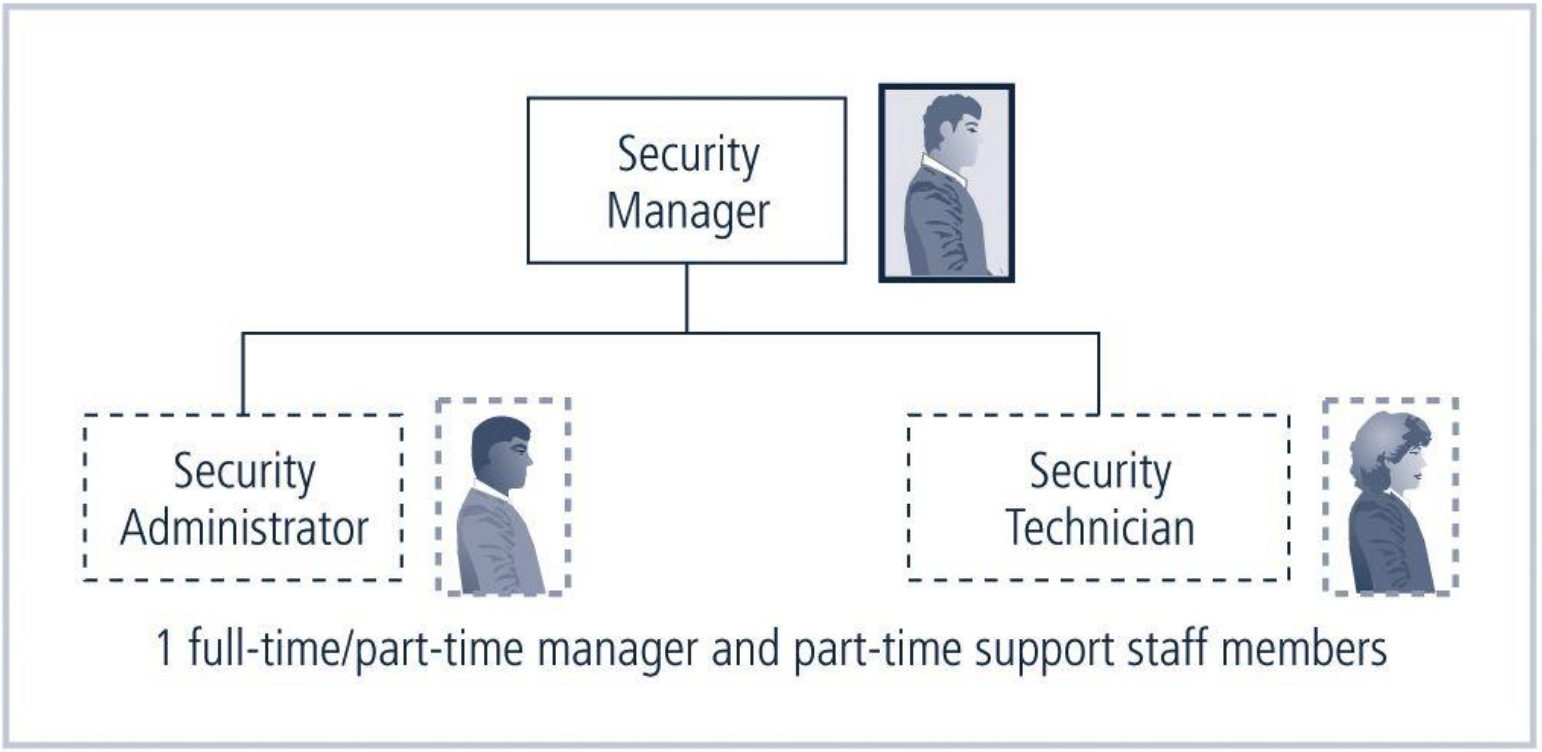
- May be large enough to implement multi-tiered approach to security with fewer dedicated groups and more functions assigned to each group
- Medium-sized organizations tend to ignore some security functions

InfoSec Staffing in a Medium Organization



Information Security Staffing in a Medium-Sized Organization

InfoSec Staffing in a Smaller Organization



Information Security Staffing in a Smaller Organization

Security in Small Organizations 10-100 Computers

- Have simple, centralized IT organizational model
- Spend disproportionately more on security
- Information security in small org is often responsibility of a single security administrator
- Such organizations frequently have little in the way of formal policy, planning, or security measures
  - Commonly outsource their Web presence or electronic commerce operations
  - Security training and awareness is commonly conducted on a 1-on-1 basis

Security in Small Organizations 10-100 Computers (Continued)

- Policies are often issue-specific
- Formal security planning is often part of IT planning conducted by CIO
- To their advantage they avoid some threats precisely because of their size.
  - Threats from insiders are less likely in an environment where every employee knows every other employee

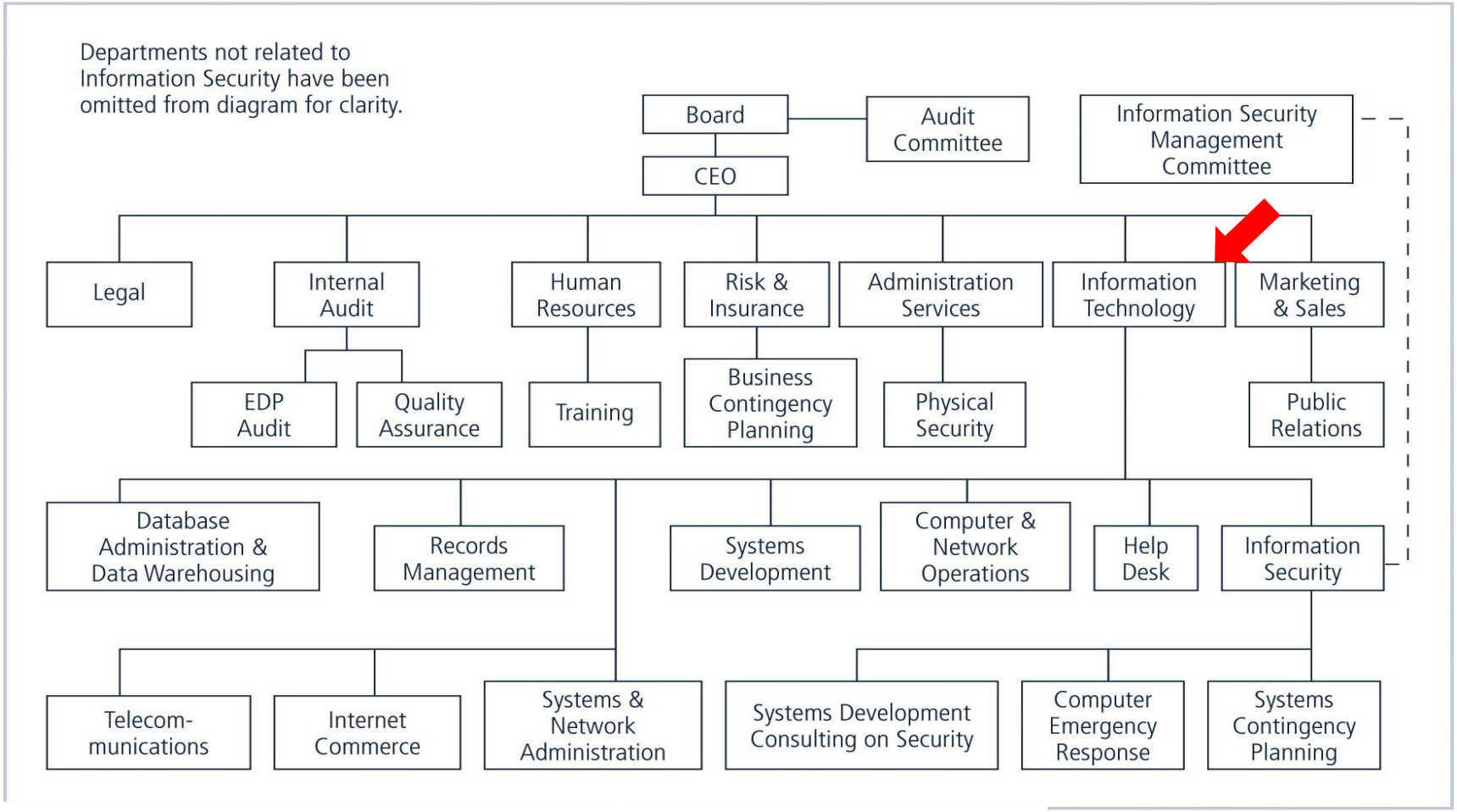
Placing Information Security Within An Organization

- In large organizations, InfoSec is often located within IT department, headed by CISO who reports directly to top computing executive, or CIO
- By its very nature, an InfoSec program is sometimes at odds with the goals and objectives of the IT department as a whole

Placing Information Security Within An Organization (Continued)

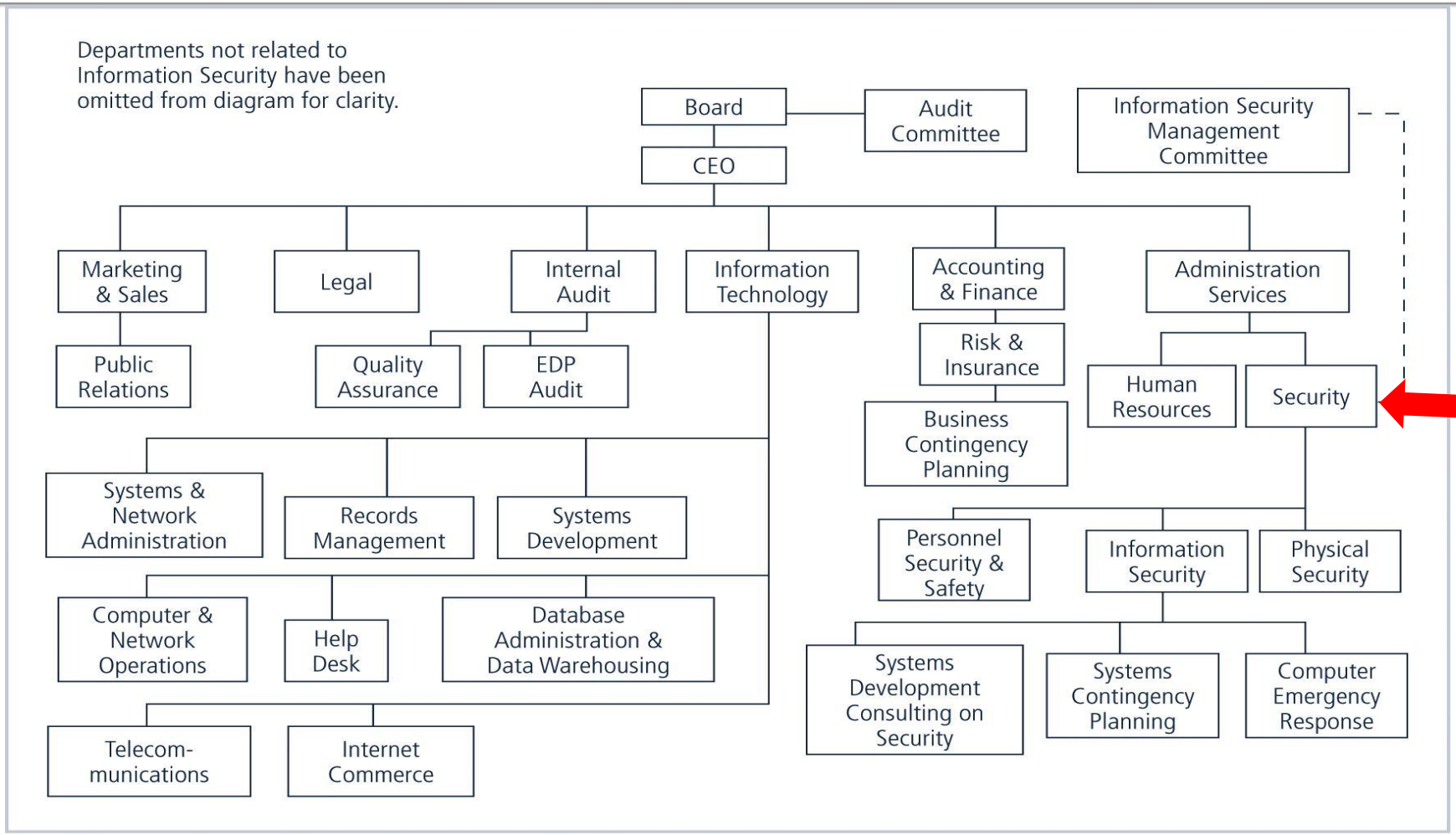
- Because the goals and objectives of CIO and CISO may come in conflict, it is not difficult to understand current movement to separate information security from IT division
- The challenge is to design a reporting structure for the InfoSec program that balances the needs of each of the communities of interest

IT Department



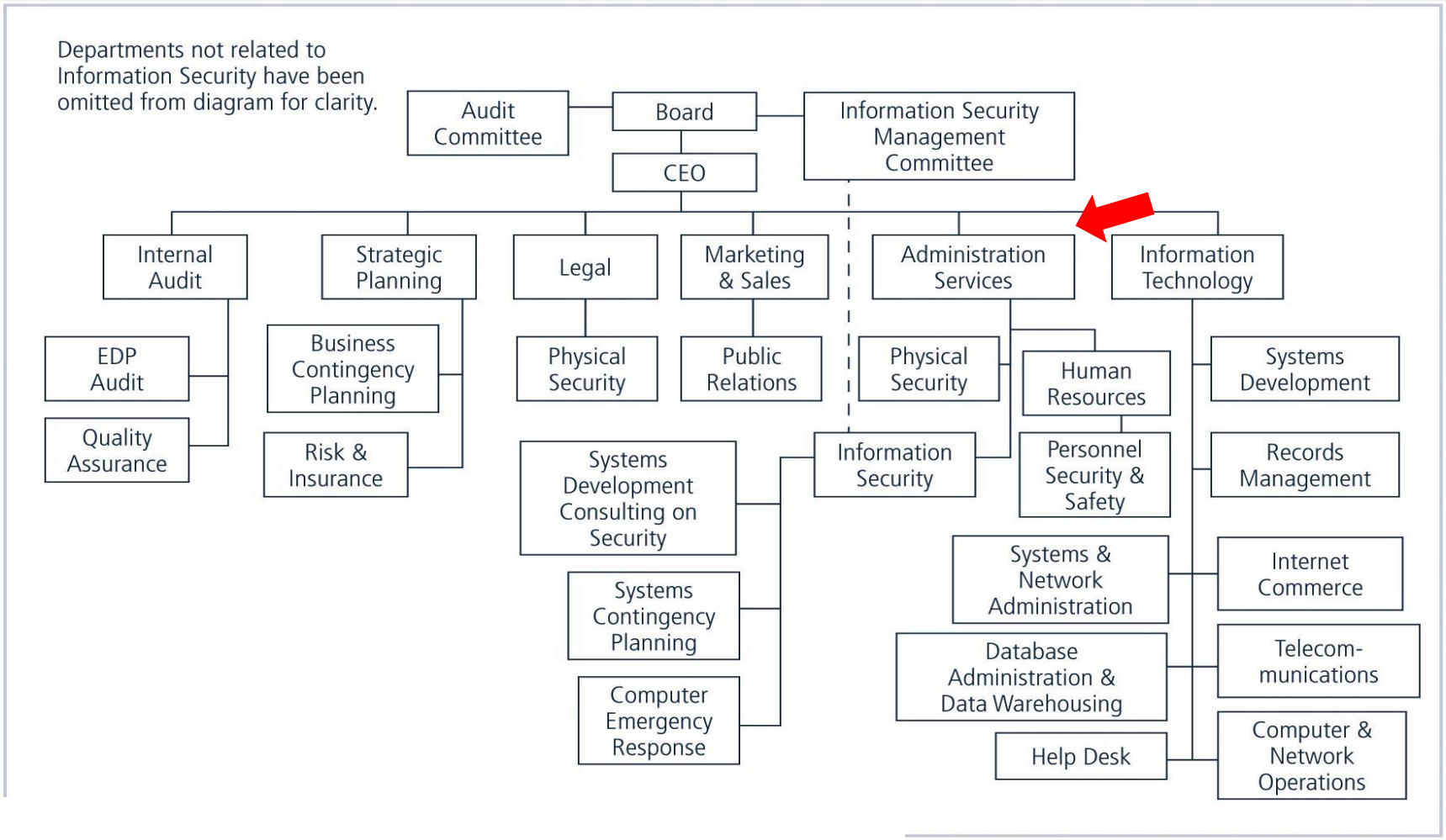
Option 1: Information Security Reports to Information Technology Department

Broadly Defined Security Department



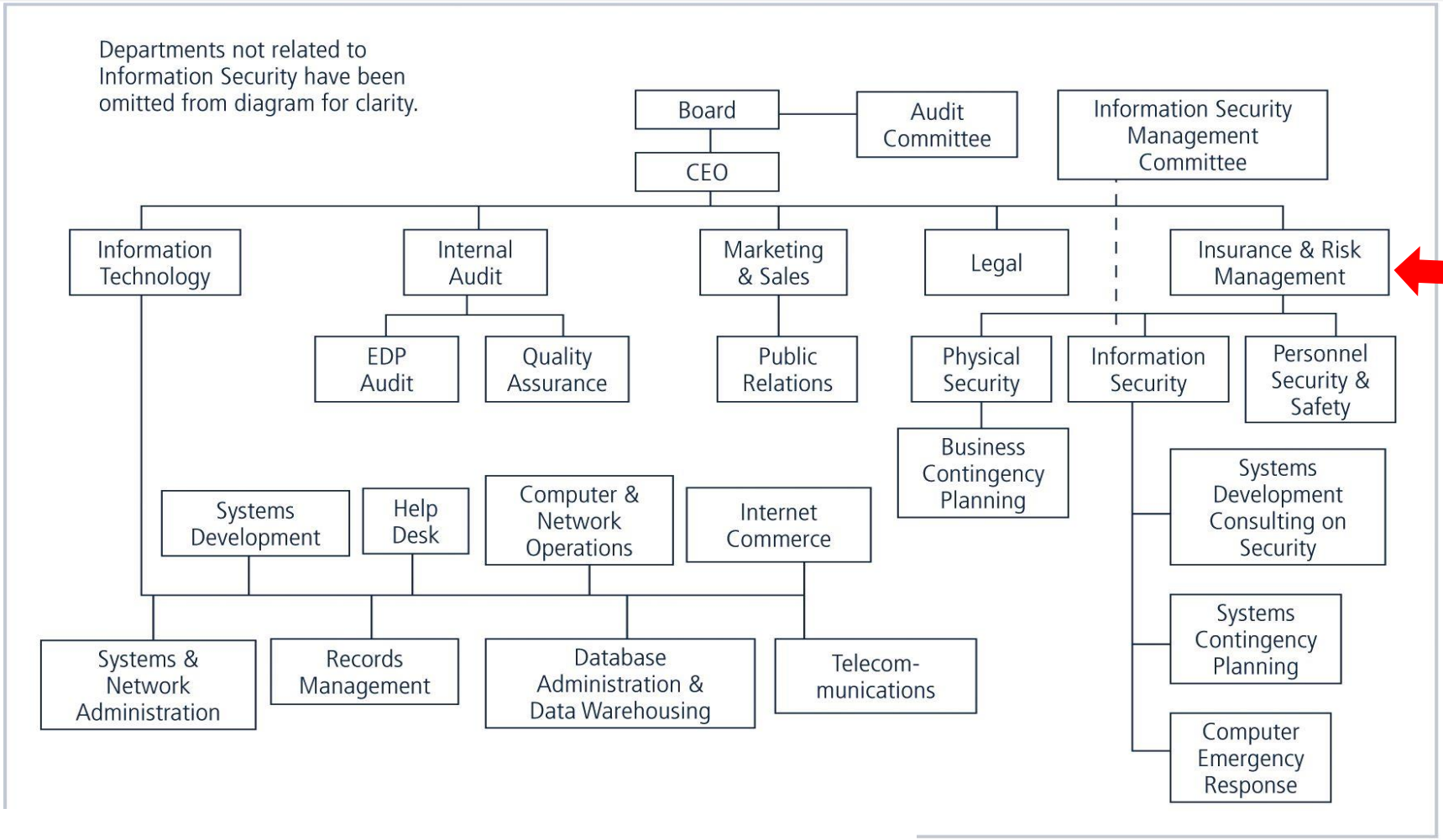
Option 2: Information Security Reports to Broadly Defined Security Department

Administrative Services Department



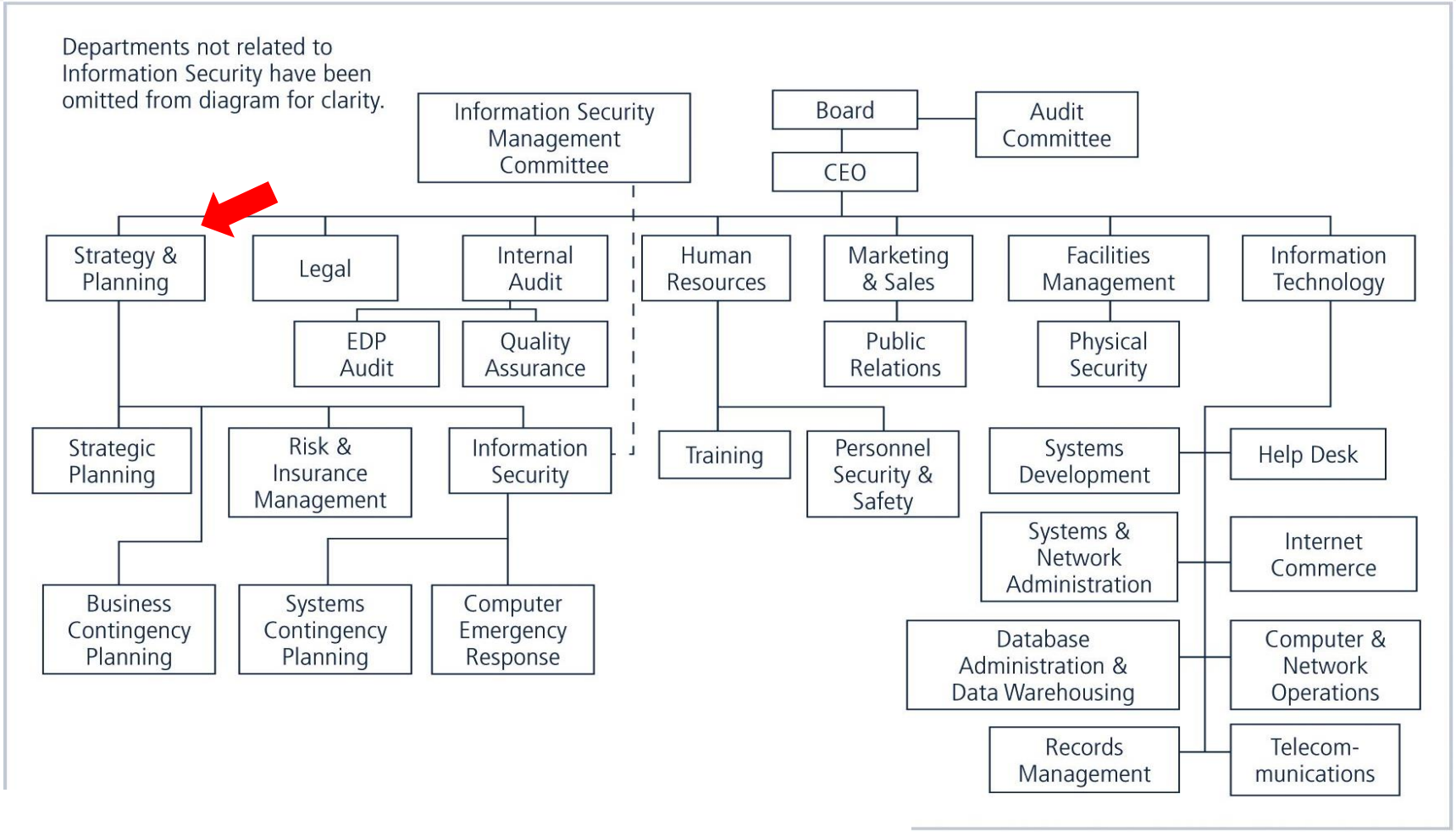
Option 3: Information Security Reports to Administrative Services Department

Insurance & Risk Mgmt Department



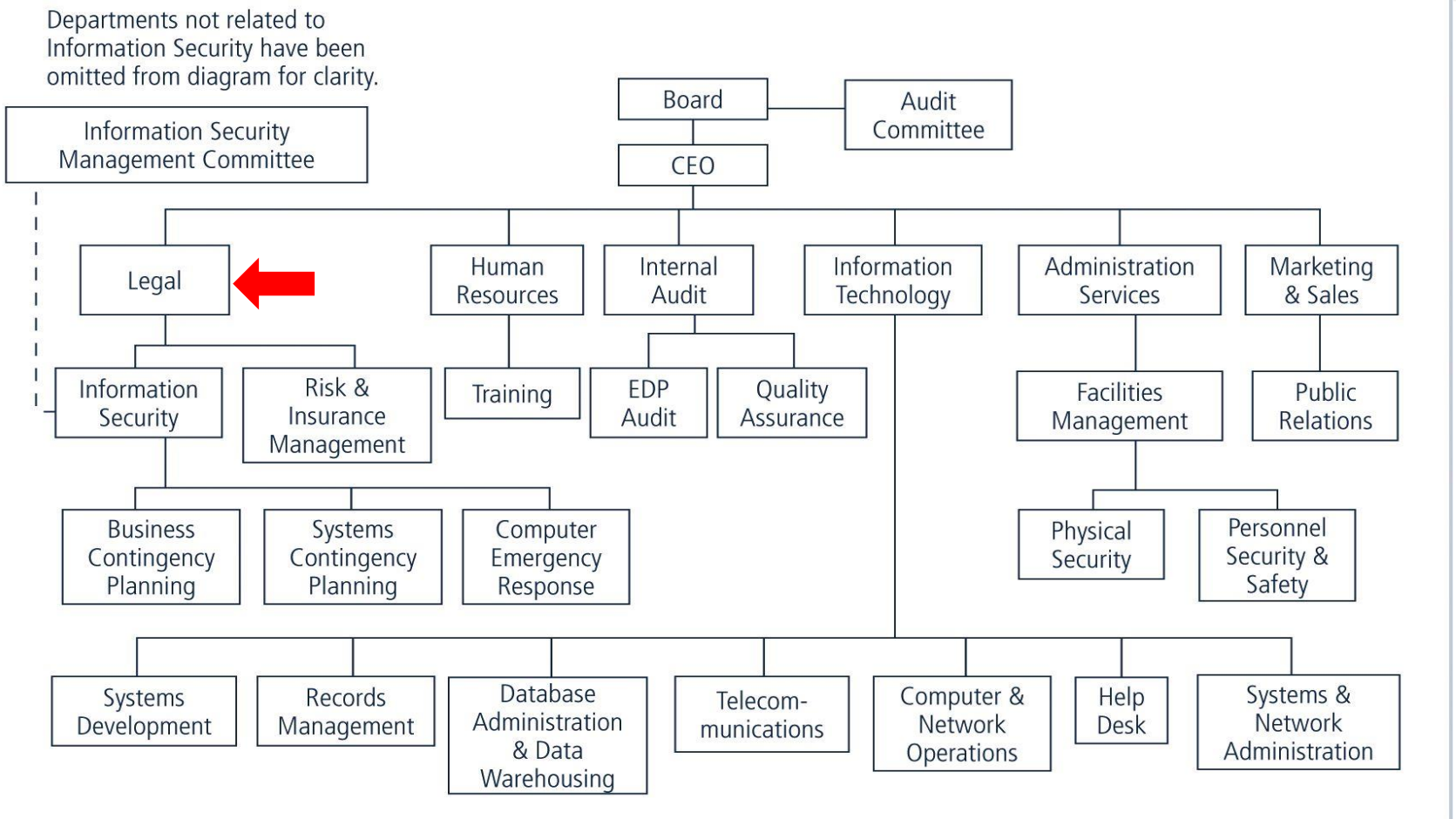
Option 4: Information Security Reports to Insurance and Risk Management Department

Strategy & Planning Department



Option 5: Information Security Reports to Strategy and Planning Department

Legal Department



Option 6: Information Security Reports to Legal Department

Other Options

- Option 7: Internal Audit
- Option 8: Help Desk
- Option 9: Accounting and Finance Through IT
- Option 10: Human Resources
- Option 11: Facilities Management
- Option 12: Operations

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

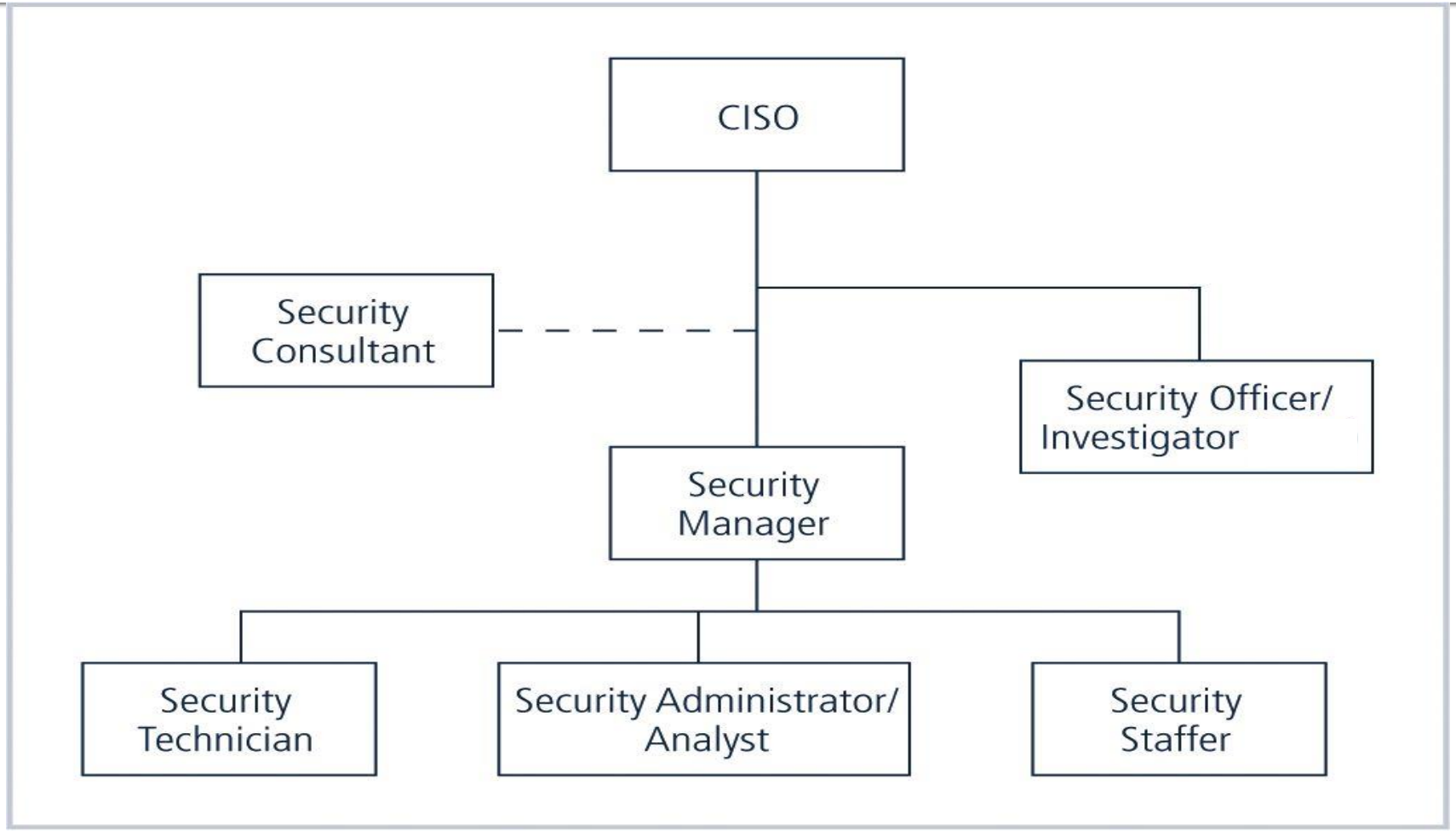
Information Security Roles

- 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

Information Security Roles



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:	Media - Videos -Newsletters -Posters, etc.	Practical Instruction - Lecture - Case study workshop - Hands-on practice	Theoretical Instruction - 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:
    - Novice
    - Intermediate
    - Advanced

Training Techniques

- Using wrong method can:
  - Hinder 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
  - 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… those who have bought the idea to help sell it
- 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 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 diligence can help indemnify 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

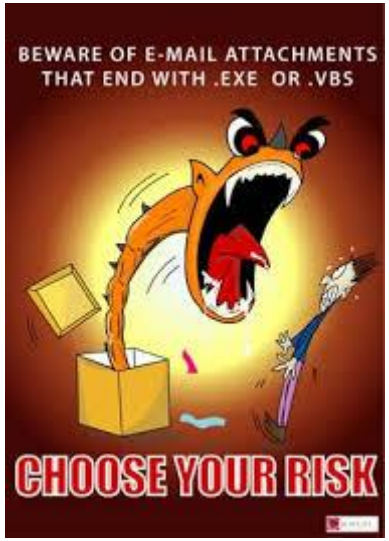
The Security Newsletter (Continued)

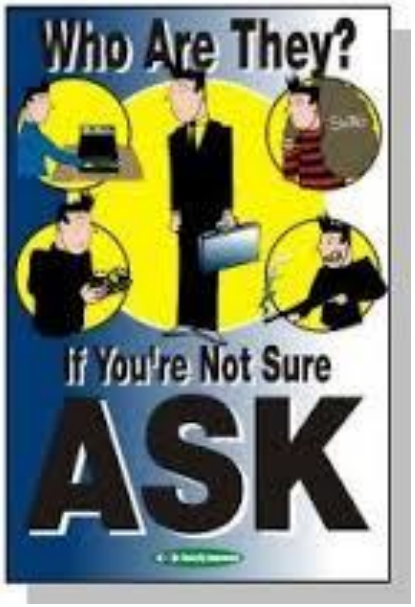
- Newsletters might include:
  - Summaries of key policies
  - Summaries of key news articles
  - A calendar of security events, including training sessions, presentations, and other activities
  - Announcements relevant to information security
  - How-to's

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

Security Posters

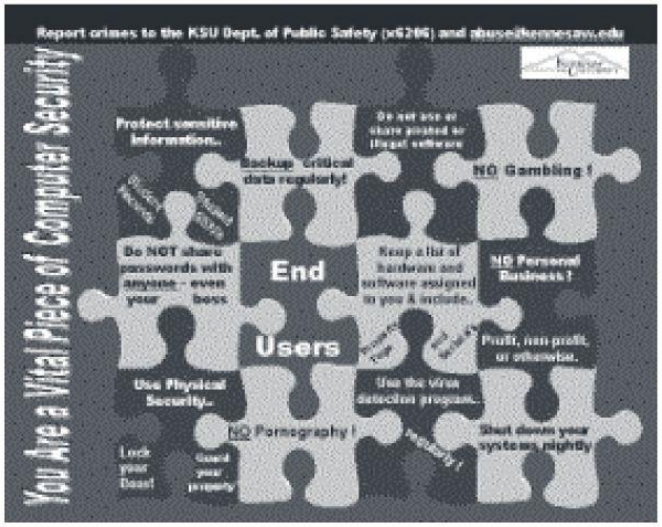




The Trinket Program

- 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

Security 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:
  - 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
  - information security week/day

Practical Group Assignments

- Develop a security background check program.
- Develop a security awareness plan / program.
- Develop a security training plan / program
- Develop an information security plan.
- Review and propose a security organization redesign.
- Develop a security hiring plan.
  - Write a job description for a security position.
  - Write an advertisement for a security job.

Summary

- Organizing for Security
- Placing Information Security Within An Organization
- Components of the Security Program
- Information Security Roles and Titles
- Implementing Security Education, Training, and Awareness Programs