TEL2813/IS2820
Security Management

Developing the Security Program

Jan 27, 2005

Introduction

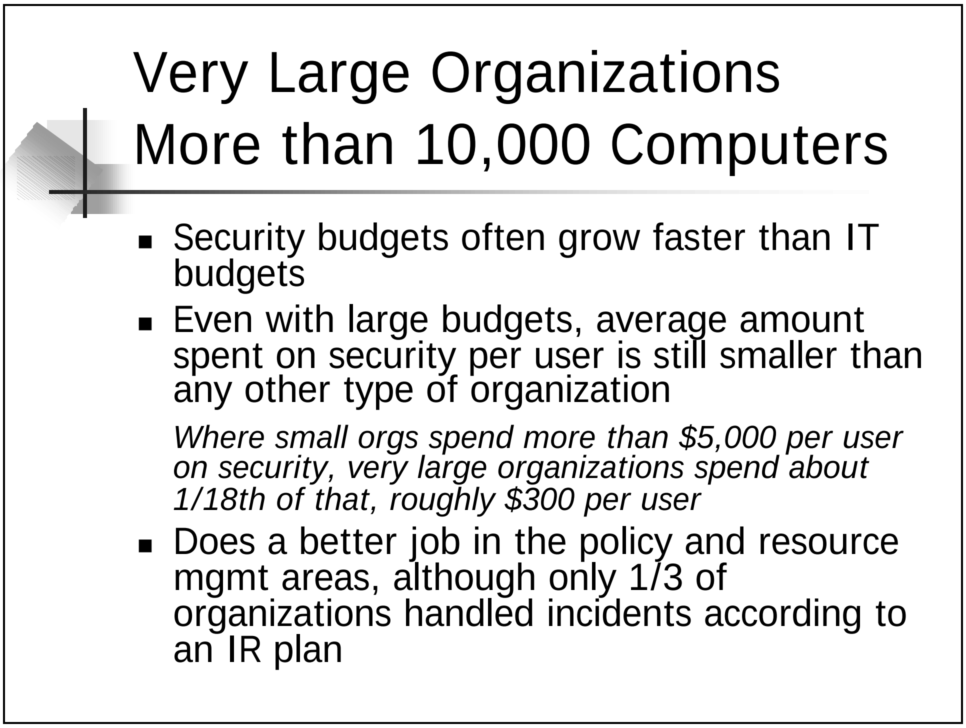
- Some organizations use security programs
  - to describe the entire set of personnel, plans, policies, and initiatives related to information security
- Information security program
  - used here to describe the structure and organization of the effort that contains risks to the information assets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

Security in Large Organizations

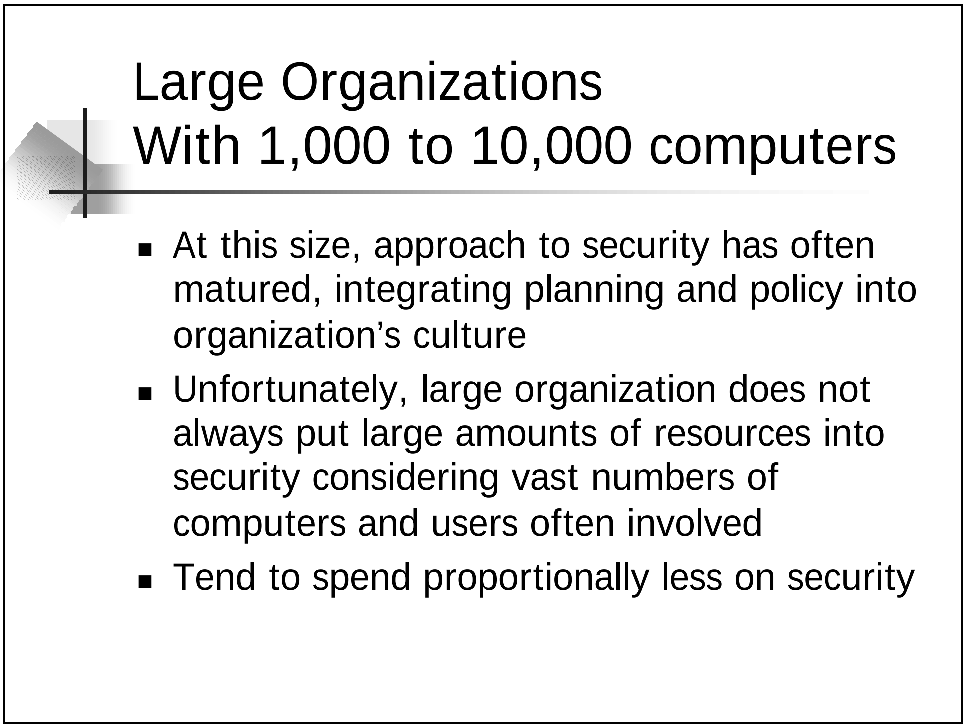
- Information security departments in large organizations tend to form and re-form internal groups to meet long-term challenges even as they handle day-to-day security operations
- Functions are likely to be split into groups
- In contrast, smaller organizations typically create fewer groups, perhaps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



Very Large Organizations More than 10,000 Computers

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

  Where small orgs spend more than $5,000 per user on security, very large organizations spend about 1/18th of that, roughly $300 per user
- Does a better job in the policy and resource mgmt areas, although only 1/3 of organizations handled incidents according to an IR plan



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 does 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

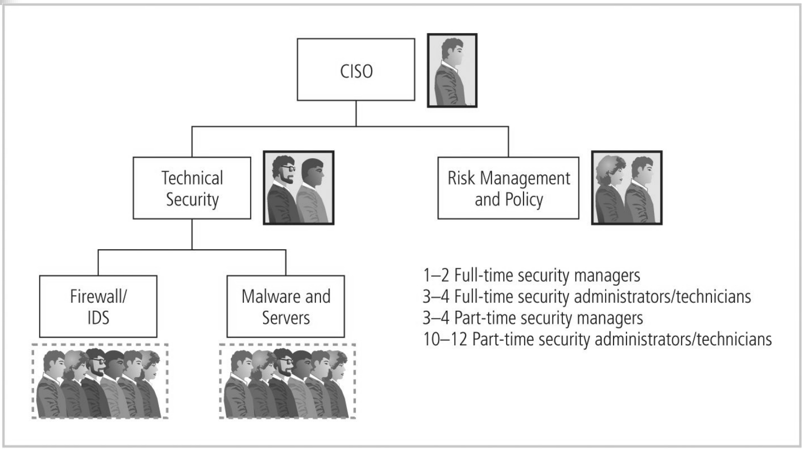
Security in Large Organizations

- An approach: separate functions into 4 areas:
  - Functions performed by non-technology business units outside of IT
    - Legal; training
  - Functions performed by IT groups outside of information security area
    - Network/systems security administrator
  - Functions performed within information security department as customer service
    - Risk assessment; systems testing; incident response
  - Functions performed within the information security department as compliance
    - Policy; compliance

Responsibilities in Large Organizations

- Remains CISO's responsibility to see that
  - information security functions are adequately performed somewhere 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

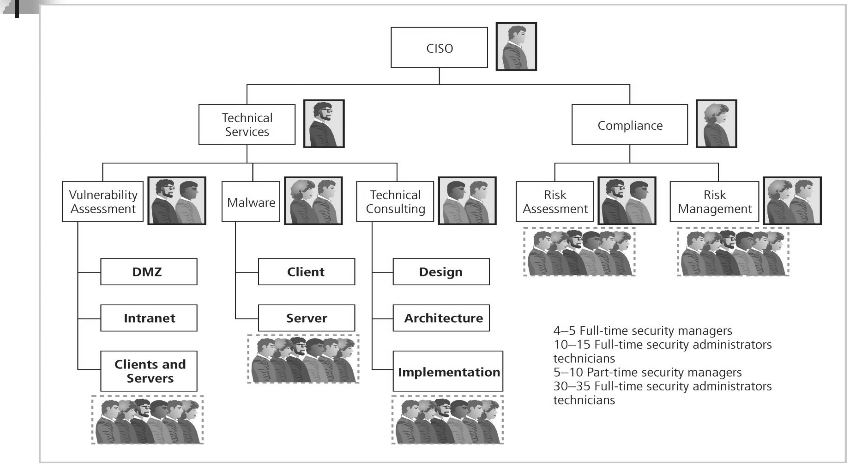
Typical Information Security Staffing in a Large Organization



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

FIGURE 5-1 Information Security Staffing in a Large Organization

Typical 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

FIGURE 5-2 Information Security Staffing in a Very Large Organization

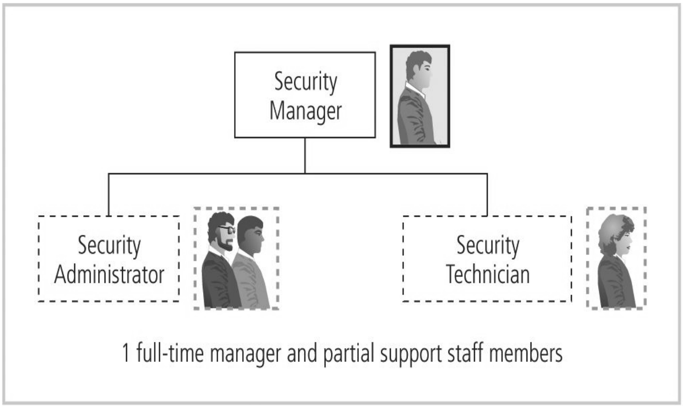
Security in Medium-Sized Organizations (100-1,000 PCs)

- 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
- Ability to set policy, handle incidents in regular manner and effectively allocate resources is, overall, worse than any other size

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

- 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

Typical InfoSec Staffing in a Medium Organization



1 full-time manager and partial support staff members

FIGURE 5-3 Information Security Staffing in a Medium-Sized Organization

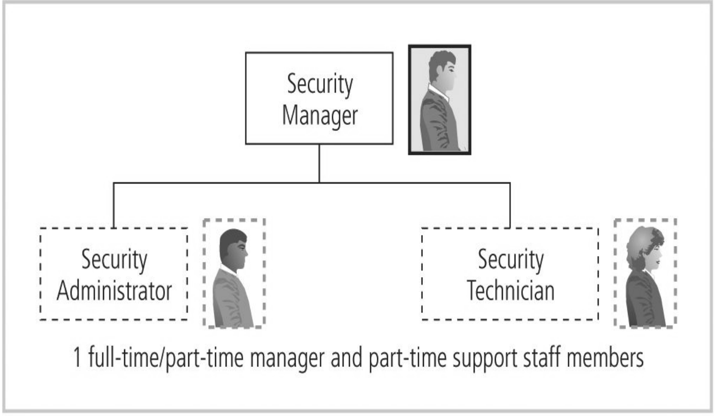
Security in Small Organizations 10-100 Computers

- 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 planning is often part of IT planning
- Threats from insiders are less likely in an environment where every employee knows every other employee

InfoSec Staffing in a Smaller Organization



Security Manager

Security Administrator

Security Technician

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

FIGURE 5-4 Information Security Staffing in a Smaller Organization

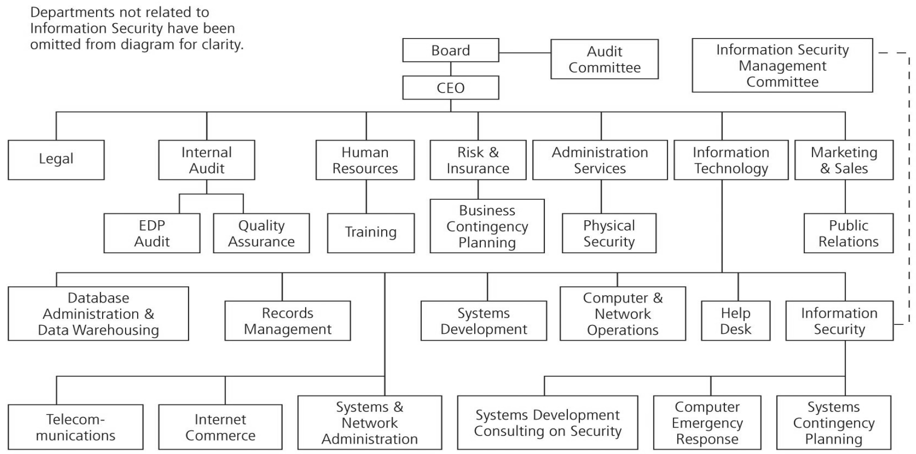
Placing Information Security Within An Organization

- 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)

- Possible conflicts between CIO/CISO goals
  - 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

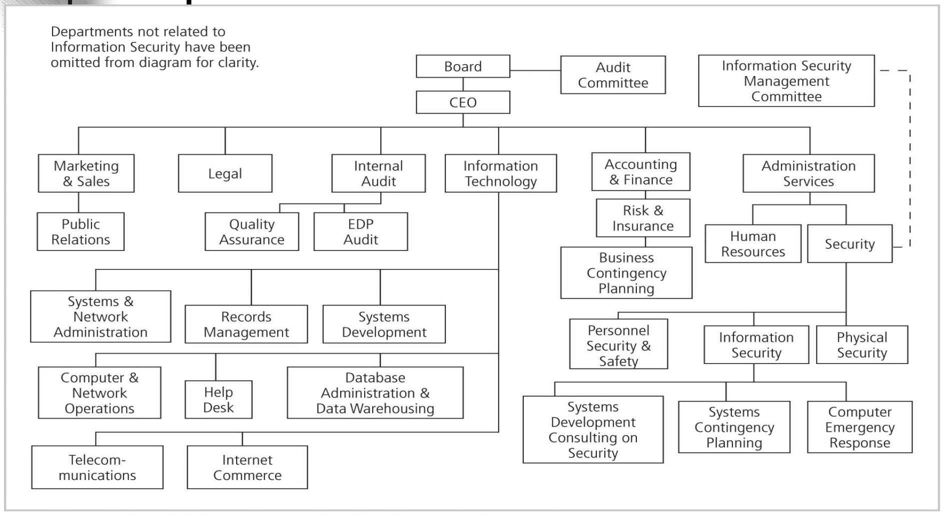
IT Department


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

From *Information Security Roles and Responsibilities Made Easy*, used with permission.

FIGURE 5-5 **Wood's Option 1: Information Security Reports to Information Technology Department**

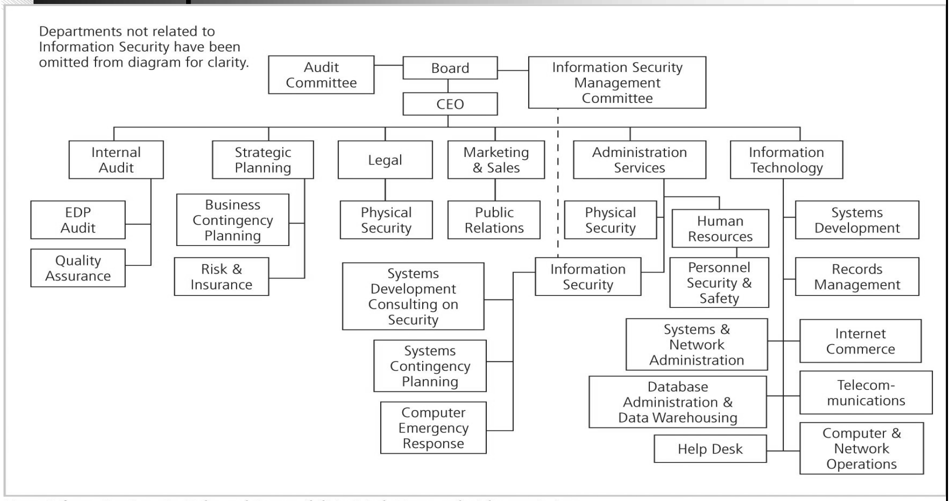
Broadly Defined Security Department


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

From *Information Security Roles and Responsibilities Made Easy*, used with permission.

FIGURE 5-6 **Wood's Option 2: Information Security Reports to Broadly Defined Security Department**

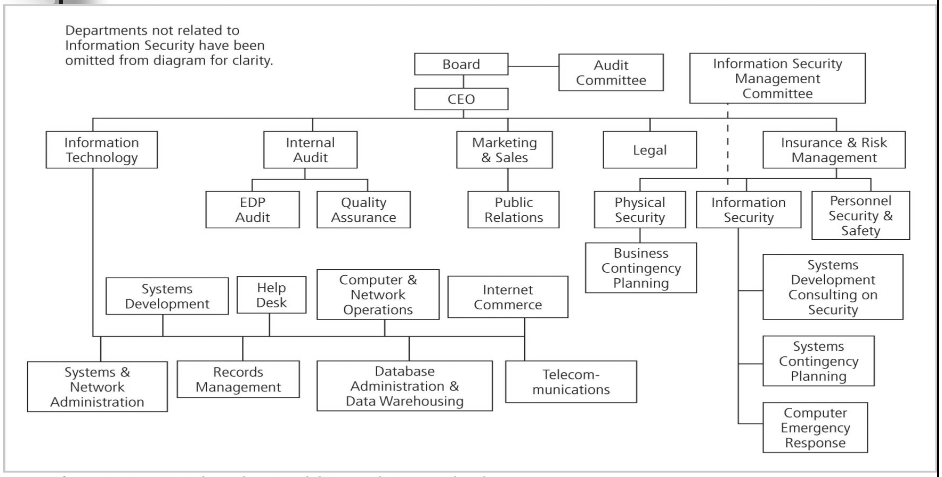
Administrative Services Department


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

From *Information Security Roles and Responsibilities Made Easy*, used with permission.

FIGURE 5-7 Wood's Option 3: Information Security Reports to Administrative Services Department

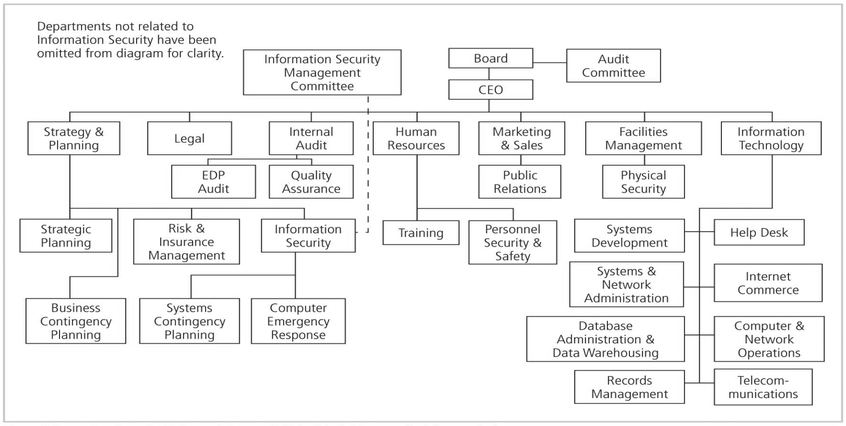
Insurance & Risk Mgmt Department


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
Help Desk
Computer & Network Operations
Internet Commerce
Systems Development Consulting on Security
Systems Contingency Planning
Systems & Network Administration
Records Management
Database Administration & Data Warehousing
Telecom-munications
Computer Emergency Response

From *Information Security Roles and Responsibilities Made Easy*, used with permission.

FIGURE 5-8 Wood's Option 4: Information Security Reports to Insurance and Risk Management Department

Strategy & Planning Department

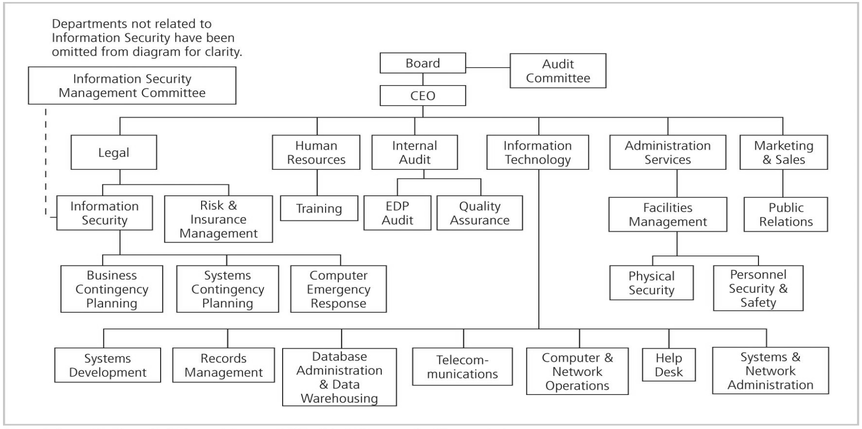

Departments not related to Information Security have been omitted from diagram for clarity.
Information Security Management Committee
Board
Audit Committee
CEO
Strategy & Planning
Legal
Internal Audit
Human Resources
Marketing & Sales
Facilities Management
Information Technology
EDP Audit
Quality Assurance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

From *Information Security Roles and Responsibilities Made Easy*, used with permission.

FIGURE 5-9 **Wood's Option 5: Information Security Reports to Strategy and Planning Department**

From *Information Security Roles and Responsibilities Made Easy*, used with permission.

Legal Department


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

From *Information Security Roles and Responsibilities Made Easy*, used with permission.

FIGURE 5-10 **Wood's Option 6: Information Security Reports to Legal Department**

From *Information Security Roles and Responsibilities Made Easy*, used with permission.

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
  - NIST SP 800-14 Generally Accepted Principles for Securing Information Technology Systems
  - SP 800-12 An Introduction to Computer Security: The NIST Handbook

Information Security Roles

- Information security positions can be classified into one of three types:
  - Those that define,
    - *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.*
  - Those that build
    - *Then you have the builders. They're the real*

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

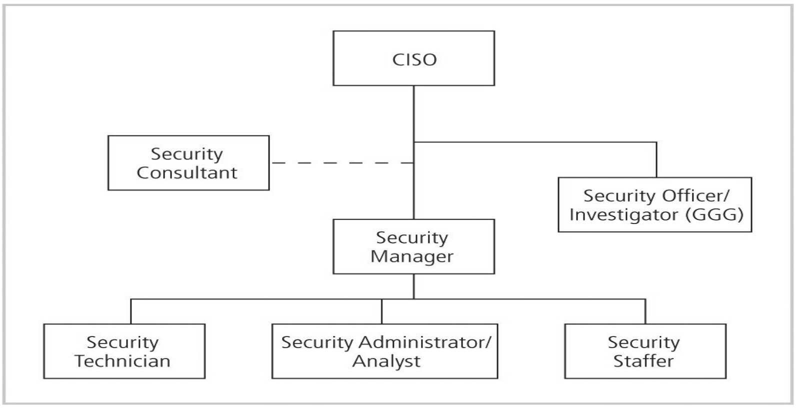


FIGURE 5-11 Information Security Roles

Integrating Security and the Help Desk

- Help desk
  - an important part of the information security team,
  - enhances the ability to identify potential problems
- User’s complaint about his or her computer,
  - 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

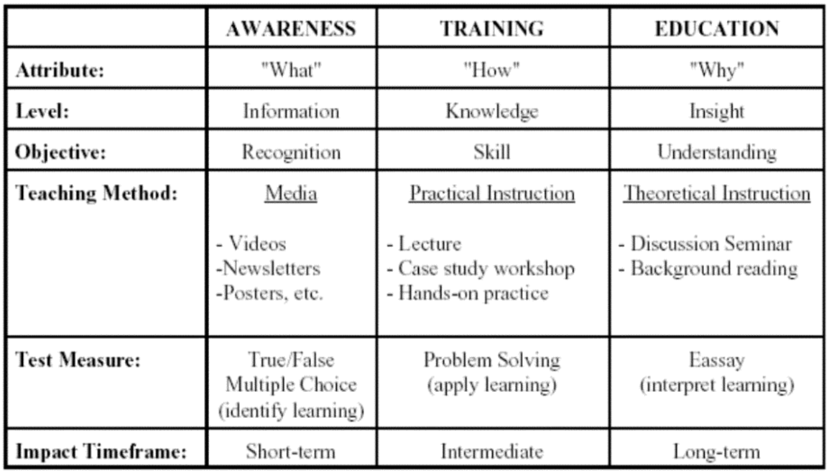
Implementing Security Education, Training, and Awareness Programs

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

Implementing SETA (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

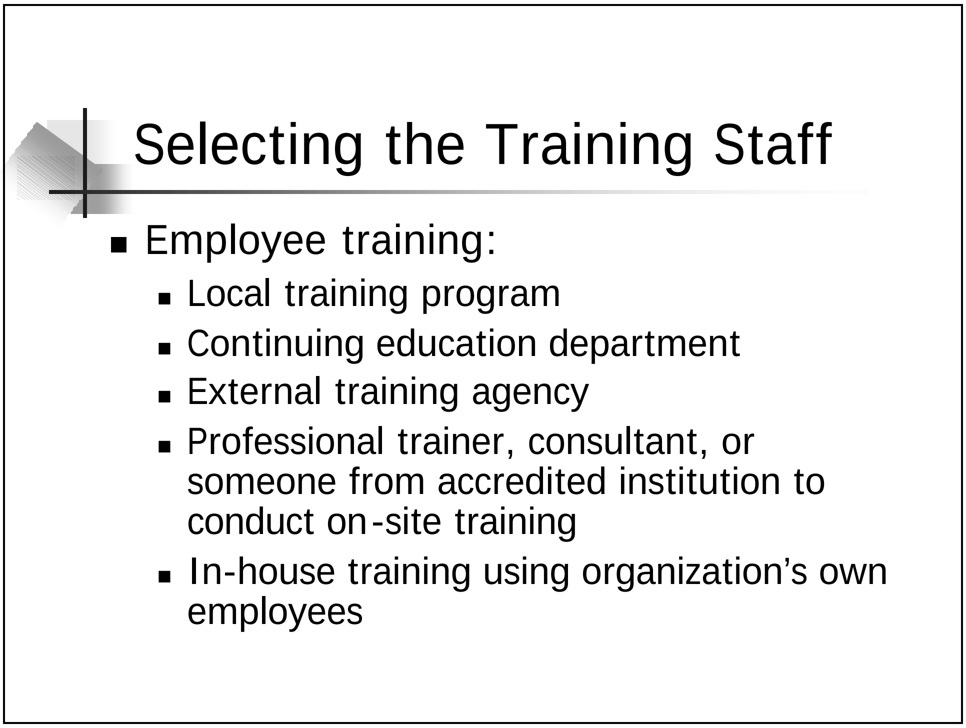
- Security training involves providing detailed information and hands-on instruction to give skills to users to perform their duties securely
- Two methods for customizing training
  - Functional background:
    - General user
    - Managerial user
    - Technical user
  - Skill level:
    - Novice
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

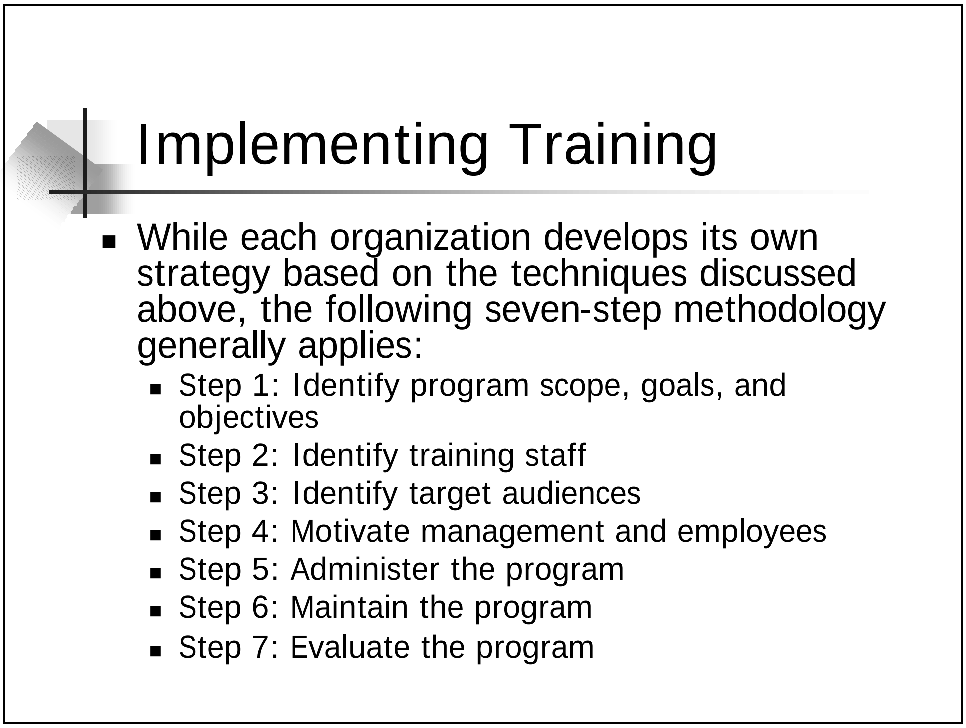
Delivery Methods

- 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)



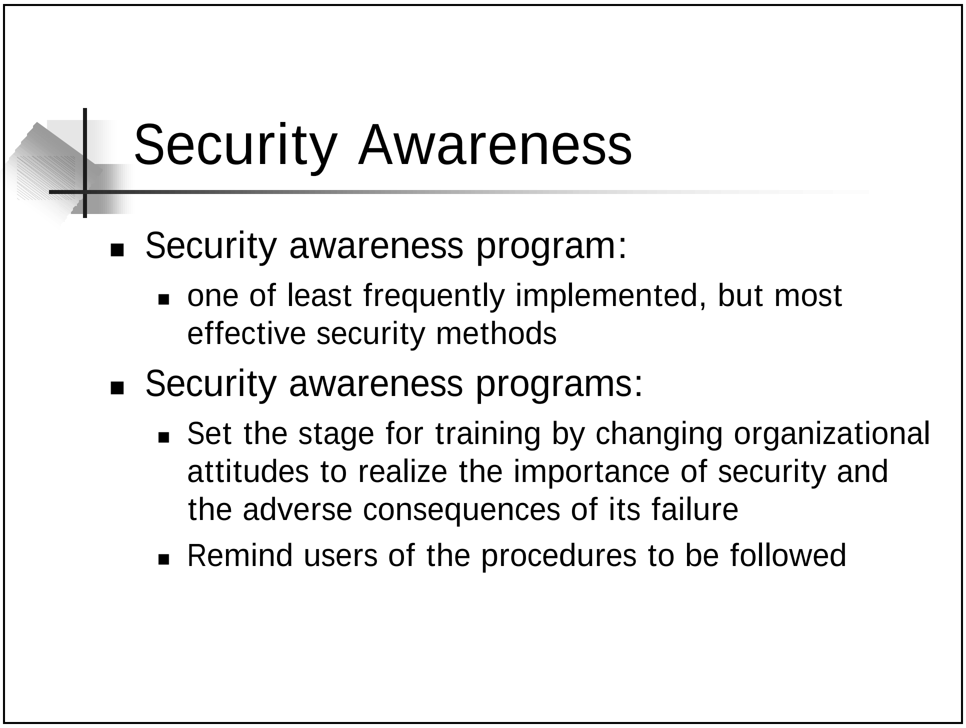
Selecting the Training Staff

- Employee training:
  - Local training program
  - 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



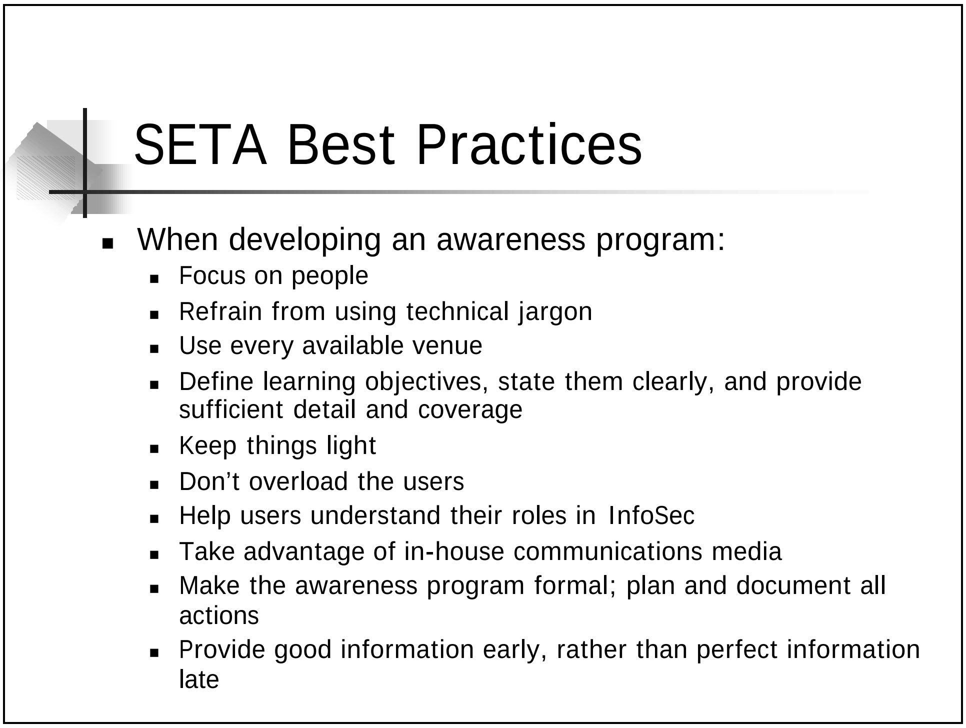
Implementing Training

- 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

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

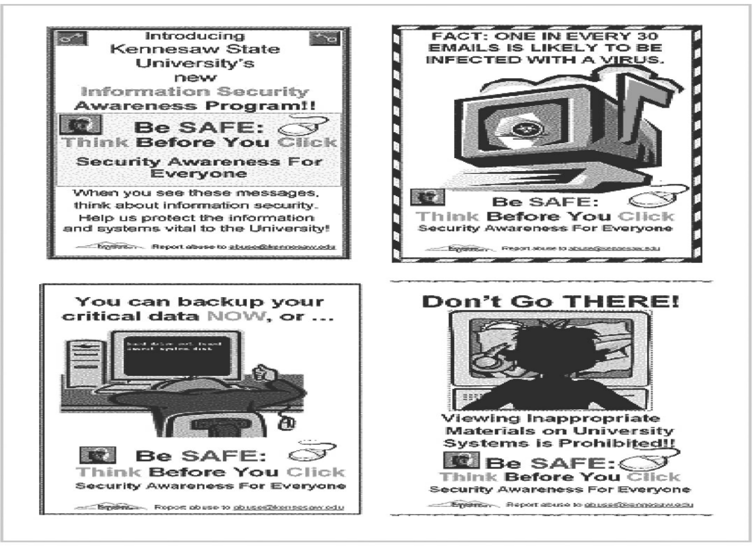

Introducing Kennesaw State University's new Information Security Awareness Program!!
Be SAFE: Think Before You Click
Security Awareness For Everyone
When you see these messages, think about information security. Help us protect the information and systems vital to the University!
Report abuse to abuse@kennesaw.edu
FACT: ONE IN EVERY 30 EMAILS IS LIKELY TO BE INFECTED WITH A VIRUS.
Be SAFE: Think Before You Click
Security Awareness For Everyone
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

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

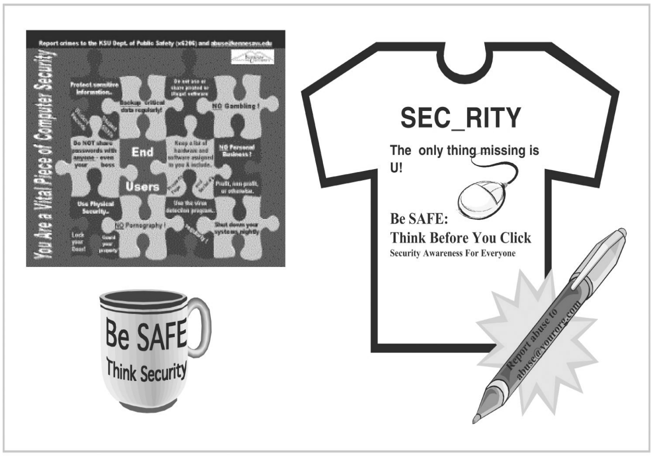

Report crimes to the KSU Dept. of Public Safety (x6206) and abuse@kennesaw.edu
You Are a Vital Piece of Computer Security
Protect sensitive information..
Do not use or share pirated or illegal software
Backup critical data regularly!
NO Gambling !
Do NOT share passwords with anyone - even your boss
End
Keep a list of hardware and software assigned to you & include..
NO Personal Business !
Users
Profit, non-profit, or otherwise.
Use Physical Security..
Use the virus detection program..
NO Pornography !
regularly!
Shut down your systems nightly
Lock your Door!
Guard your property
SEC_RITY
The only thing missing is U!
Be SAFE:
Think Before You Click
Security Awareness For Everyone
Be SAFE
Think Security
Report abuse to abuse@yourorg.com

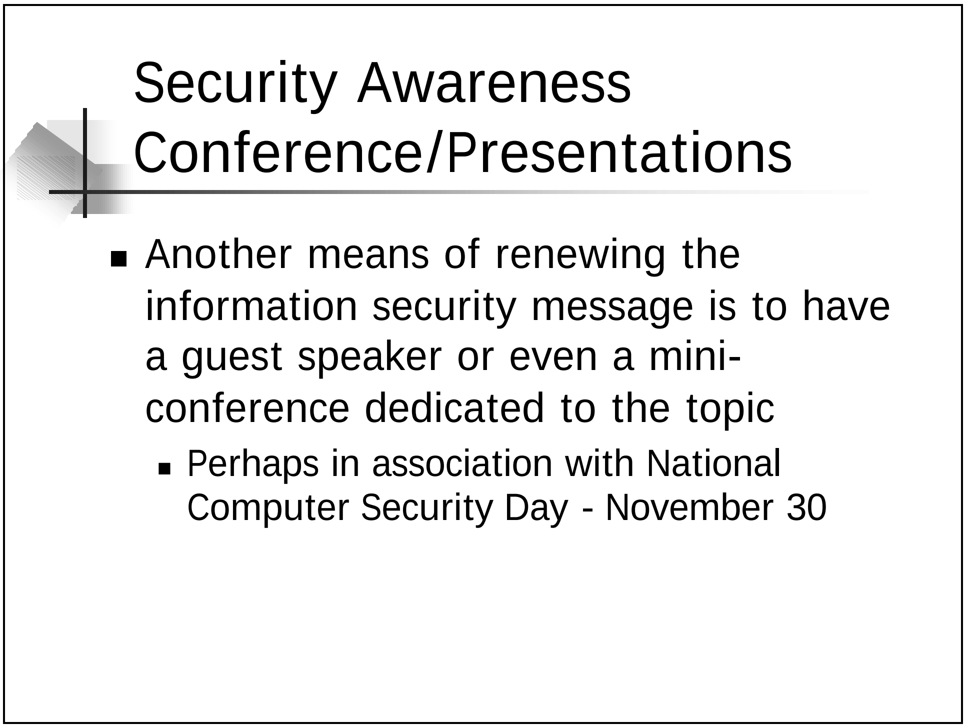
FIGURE 5-16 SETA Awareness Components: Trinkets

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