Information Security Management

Chapter 5
Developing the Security Program

Webster University
Scott Granneman

“We trained hard ... but every time
we formed up teams
we would be reorganized.
I was to learn that
we meet any new situation
by reorganizing.
And a wonderful method it can be
for creating the illusion of progress
while producing confusion, inefficiency,
and demoralization.”

-- Petronius Arbiter, 210 BCE

Upon completion of this chapter,
you should be able to:

Recognize & understand
the organizational approaches to infosec

List & describe the functional components
of the infosec program

Determine how to plan & staff
an organization's infosec program
based on its size

Evaluate the internal & external factors
that influence the activities & organization
of an infosec program

more ... →

List & describe
the typical job titles & functions
performed in the infosec program

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

Some organizations use security programs
to describe the entire set
of personnel, plans, policies, & initiatives
related to infosec

InfoSec program: used here
to describe the structure & organization
of the effort that contains risks
to the information assets of organization

Some variables that determine how to structure an infosec program are:

✓ Organizational culture

✓ Size

✓ Security personnel budget

✓ Security capital budget

“…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 & per machine
declines exponentially
as organizations grow,
leaving most handcuffed
when it comes to implementing
effective security procedures.”

InfoSec departments
in large organizations
tend to form & 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

In very large organizations
with 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

Very large organizations, however,
do a better job in the policy & resource
management areas,
although only 1/3 of organizations
handled incidents according to an IR plan

In large organizations
with 1,000 to 10,000 computers,
the approach to security has often matured,
integrating planning & policy
into organization's culture

Unfortunately, large organizations
do not always put large amounts of resources
into security
considering the vast numbers
of computers & users involved

Tend to spend
proportionally *less* on security

One approach to security
in large organizations
separates functions into 4 areas:

1. Functions performed by
non-technology business units outside IT

2. Functions performed by
IT groups outside of infosec area

3. Functions performed
within infosec dep’t as customer service

4. Functions performed
within the infosec dep’t as compliance

Remains CISO's responsibility
to see that infosec functions
are adequately performed
somewhere within the organization

Deployment of full-time security personnel
depends on a number of factors,
including sensitivity of info to be protected,
industry regulations,
& general profitability

The more money
a company can dedicate
to its personnel budget,
the more likely it is
to maintain a large infosec staff

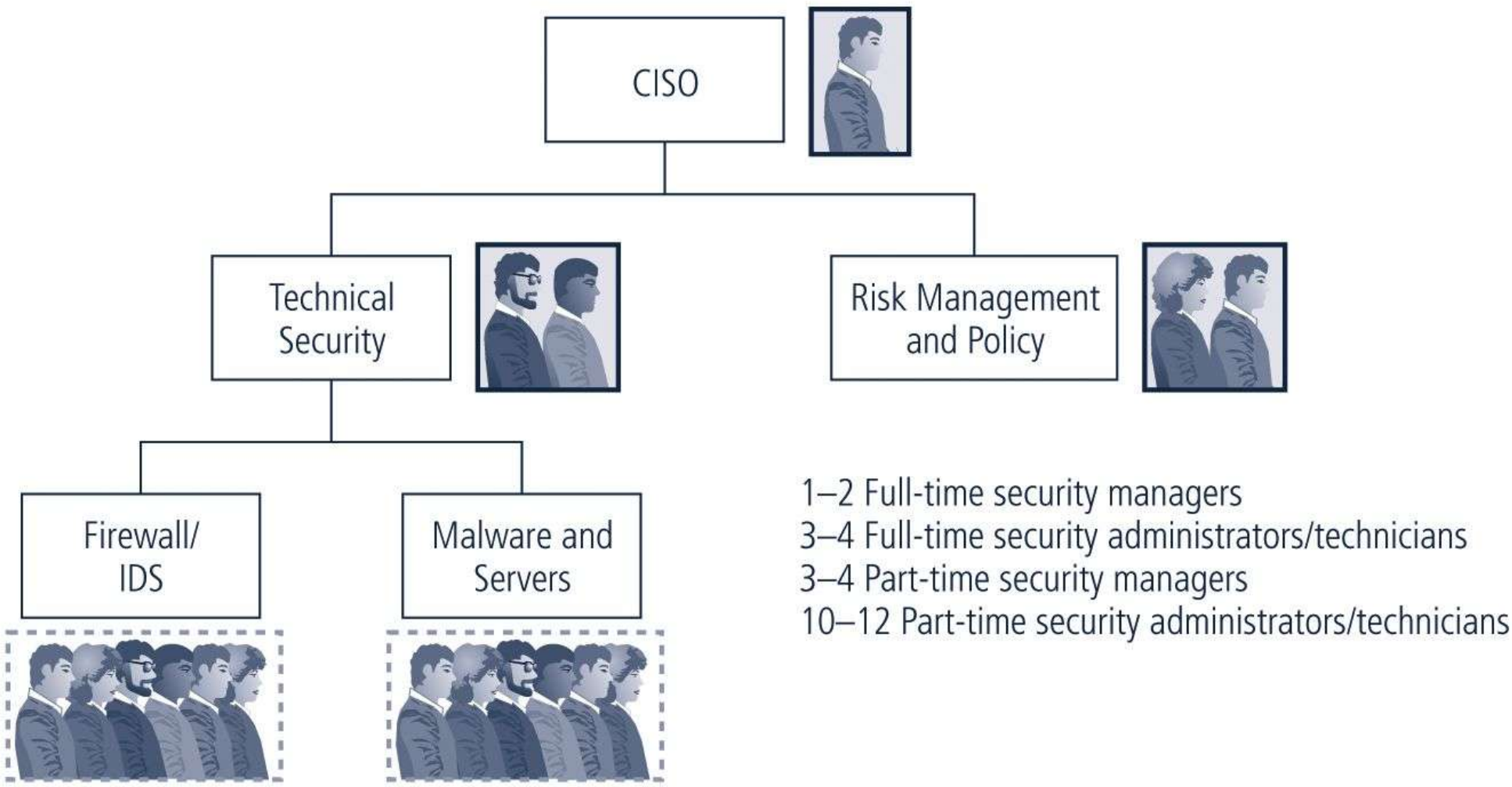


FIGURE 5-1 **Information Security Staffing in a Large Organization**

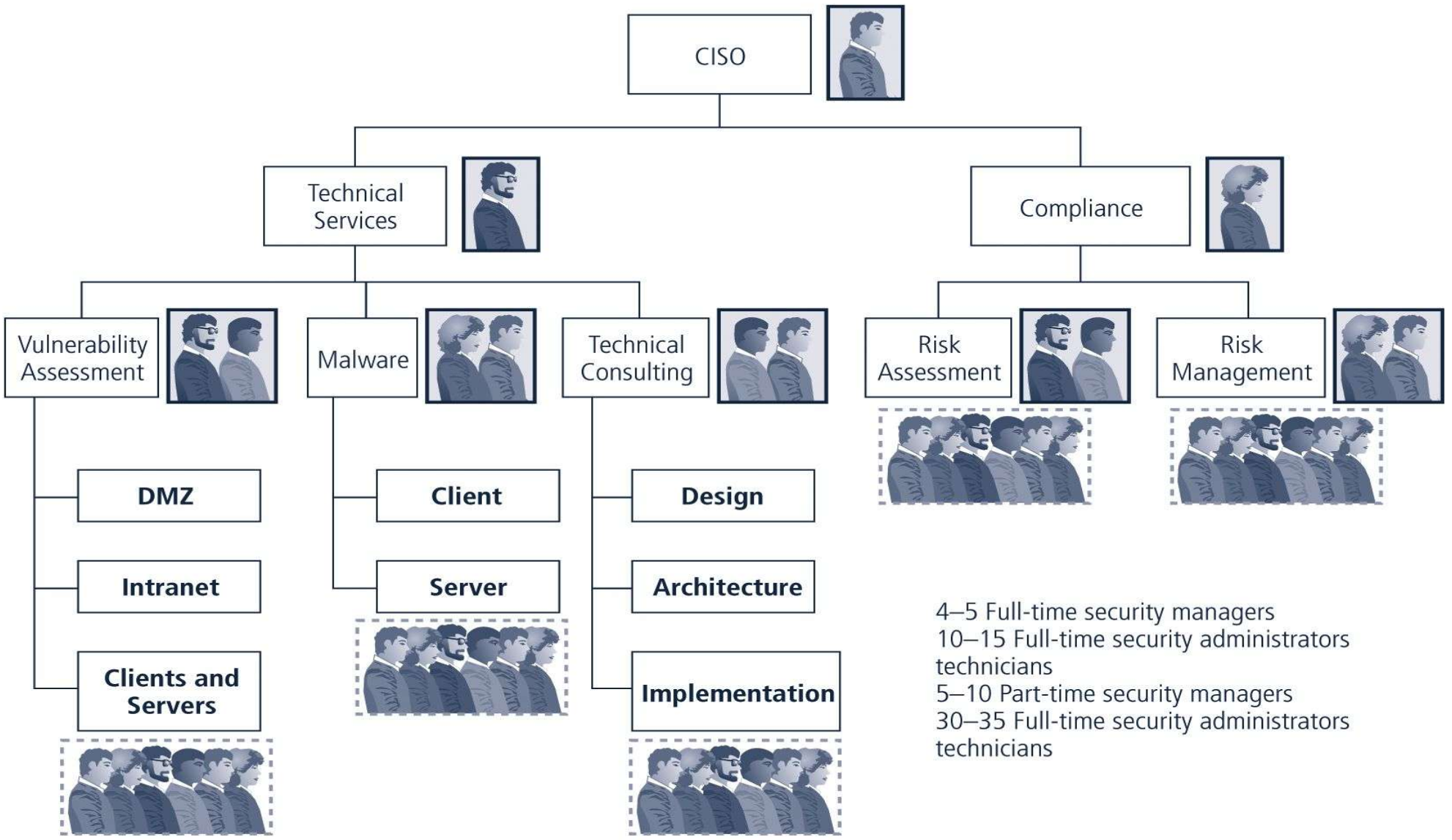


FIGURE 5-2 Information Security Staffing in a Very Large Organization

Medium-sized organizations
of 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 & practices

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

Medium-sized organizations
of 100-1,000 computers
may be large enough
to implement multi-tiered approach
to security with fewer dedicated groups
& more functions assigned to each group

Medium-sized organizations
tend to ignore some security functions

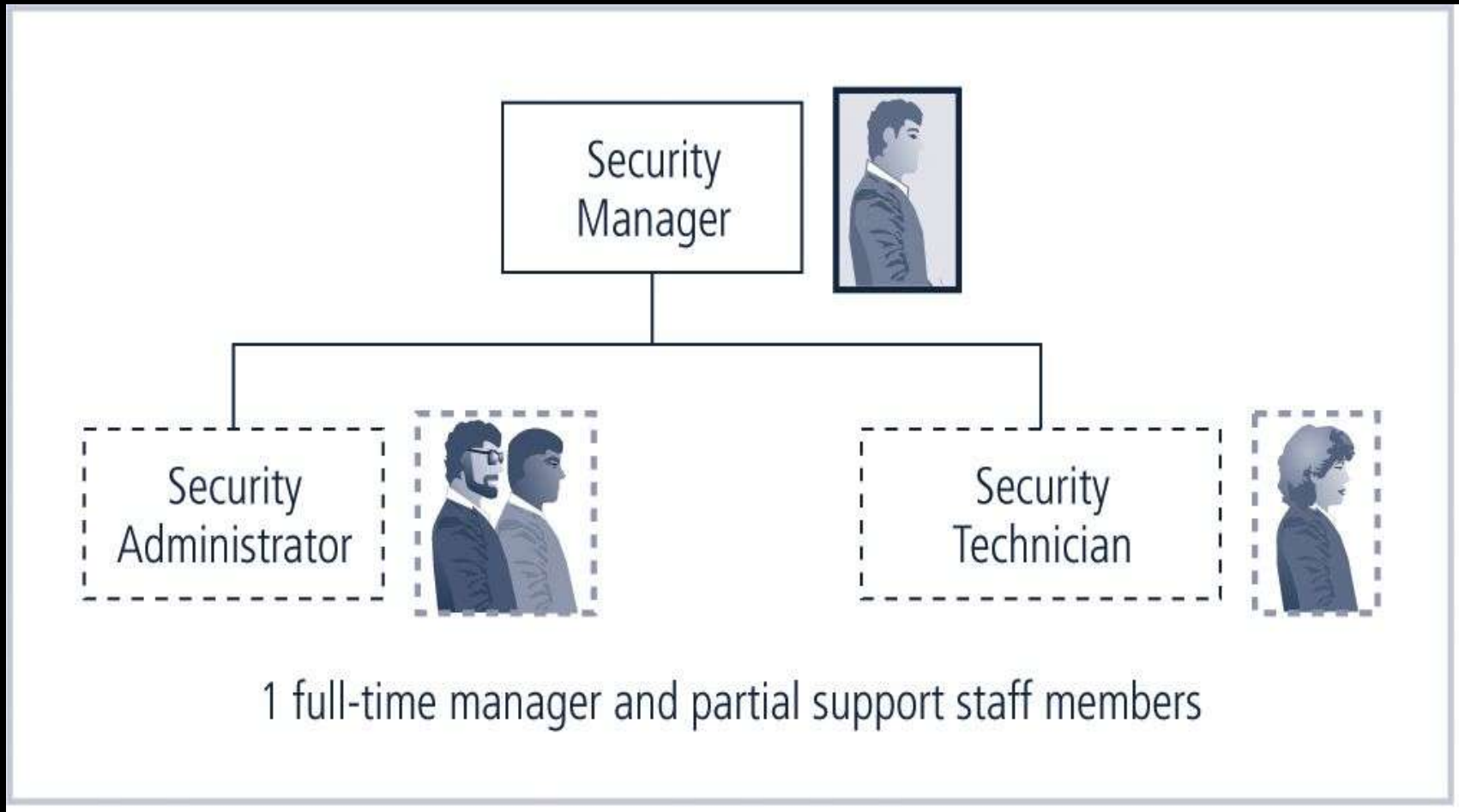


FIGURE 5-3 Information Security Staffing in a Medium-Sized Organization

Small organizations of 10-100 computers
have simple, centralized
IT organizational model

Spend disproportionately more on security

InfoSec in small org
is often responsibility
of a single
(overworked, overwhelmed)
security administrator

more ... →

Such organizations frequently
have little in the way
of formal policy, planning, or measures

Commonly outsource their Web presence
or electronic commerce operations

Security training & awareness
is commonly conducted
on a 1-on-1 basis

more ... →

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

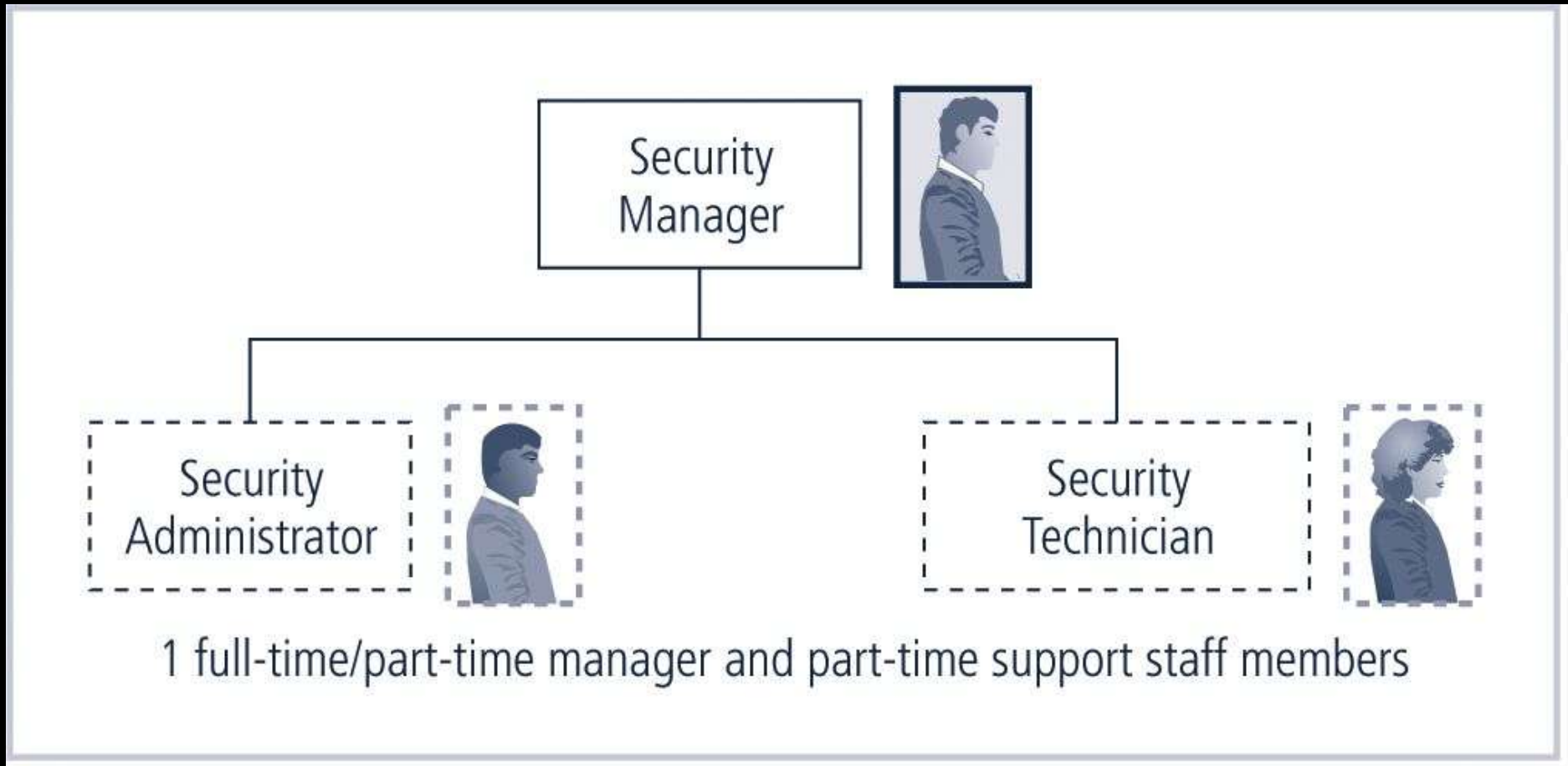


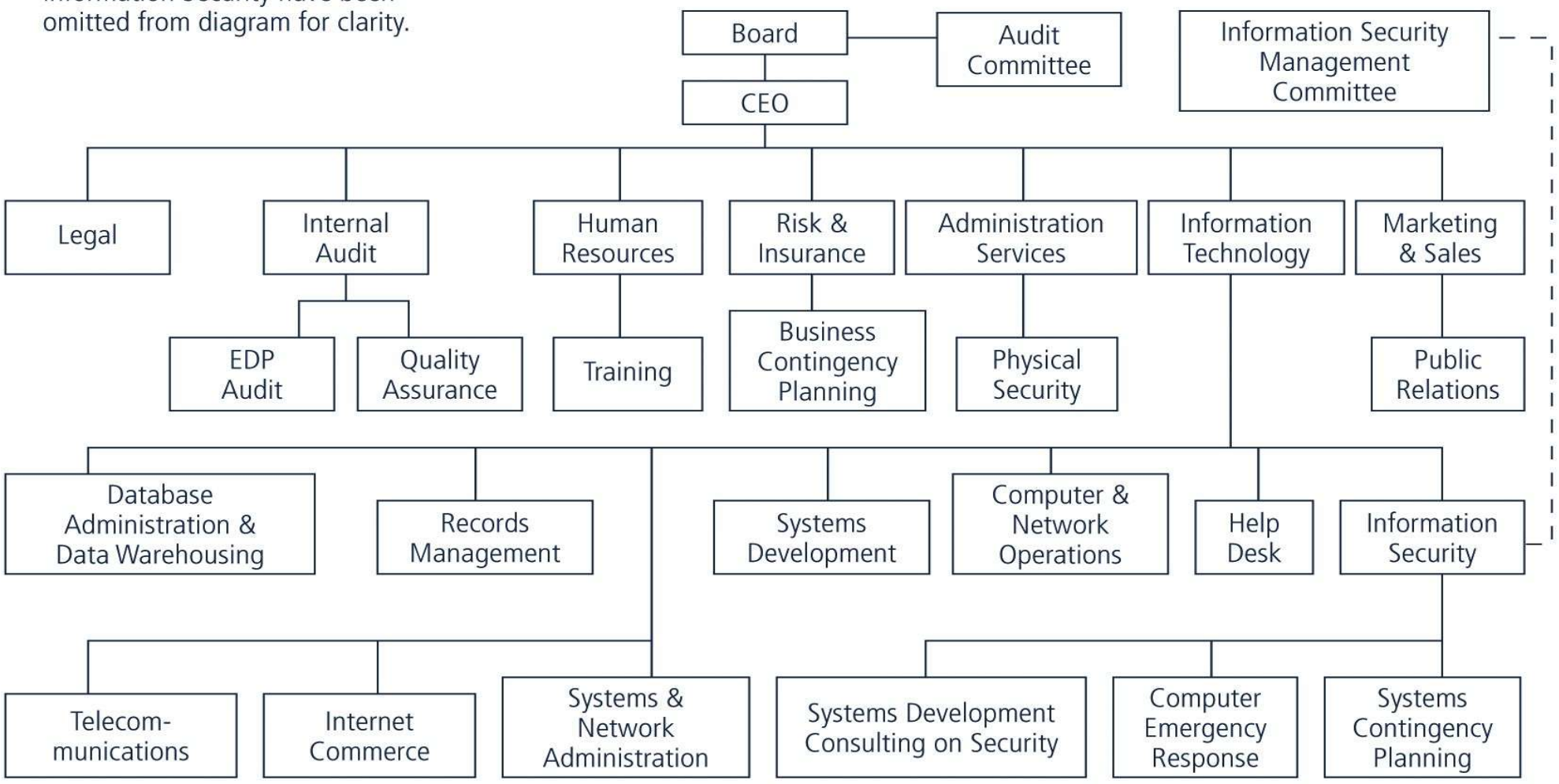
FIGURE 5-4 Information Security Staffing in a Smaller Organization

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 & objectives
of the IT department as a whole

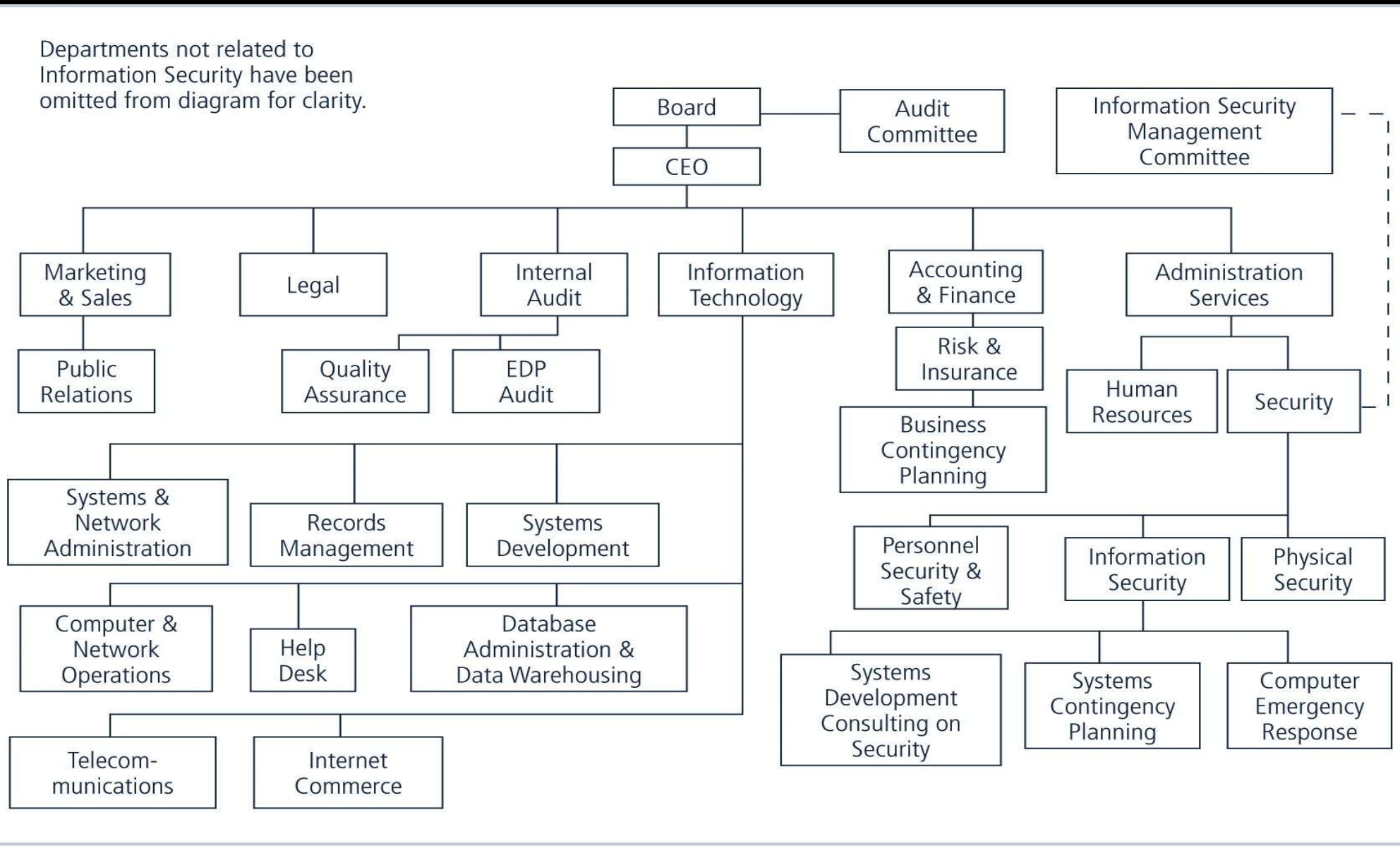
Because the goals & objectives
of CIO & CISO
may come in conflict,
it is not difficult to understand
the current movement
to separate infosec from IT division

The challenge
is to design a reporting structure
for the InfoSec program
that balances the needs
of each of the communities of interest



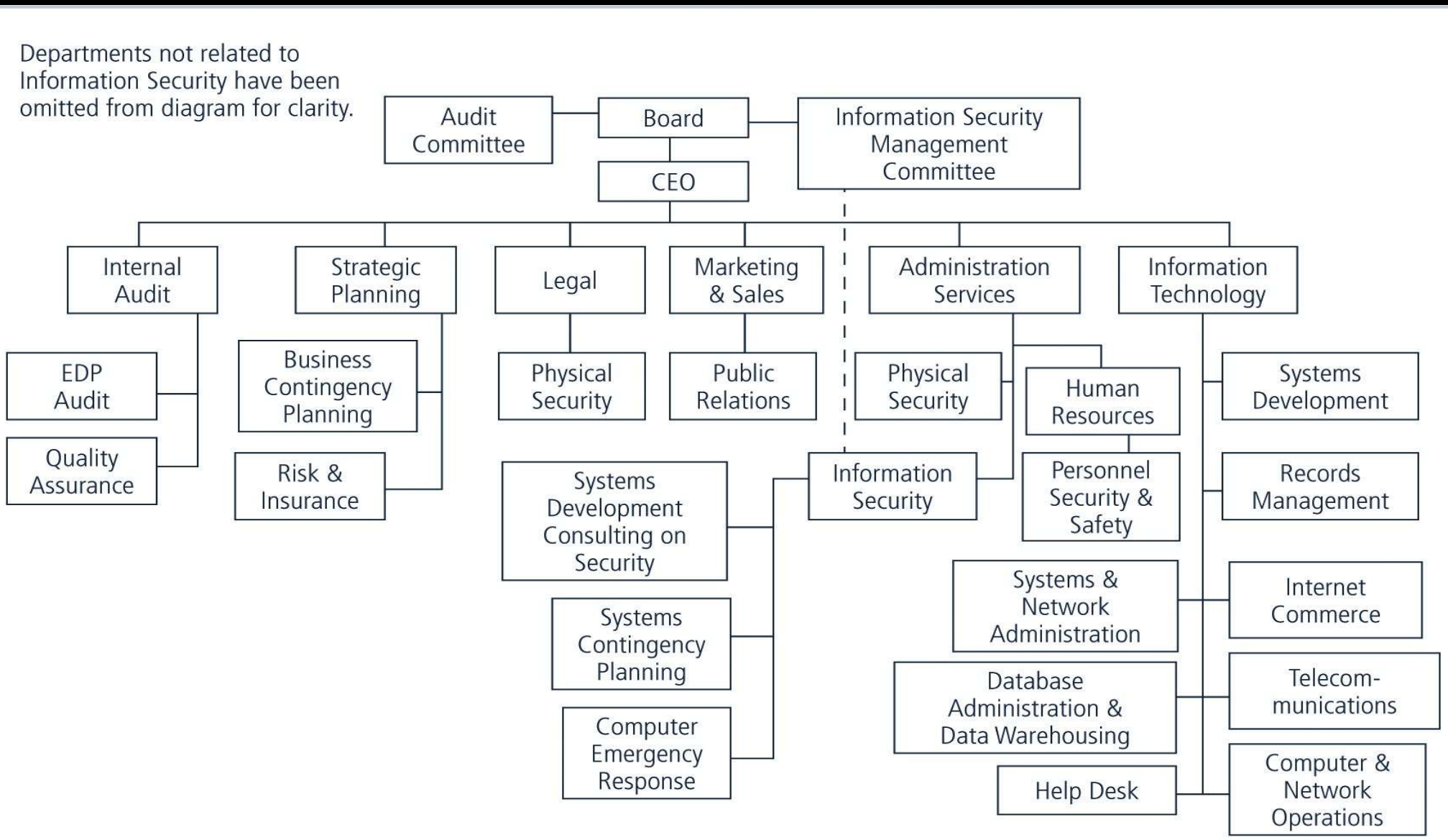
From *Information Security Roles and Responsibilities Made Easy*, used with permission.

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



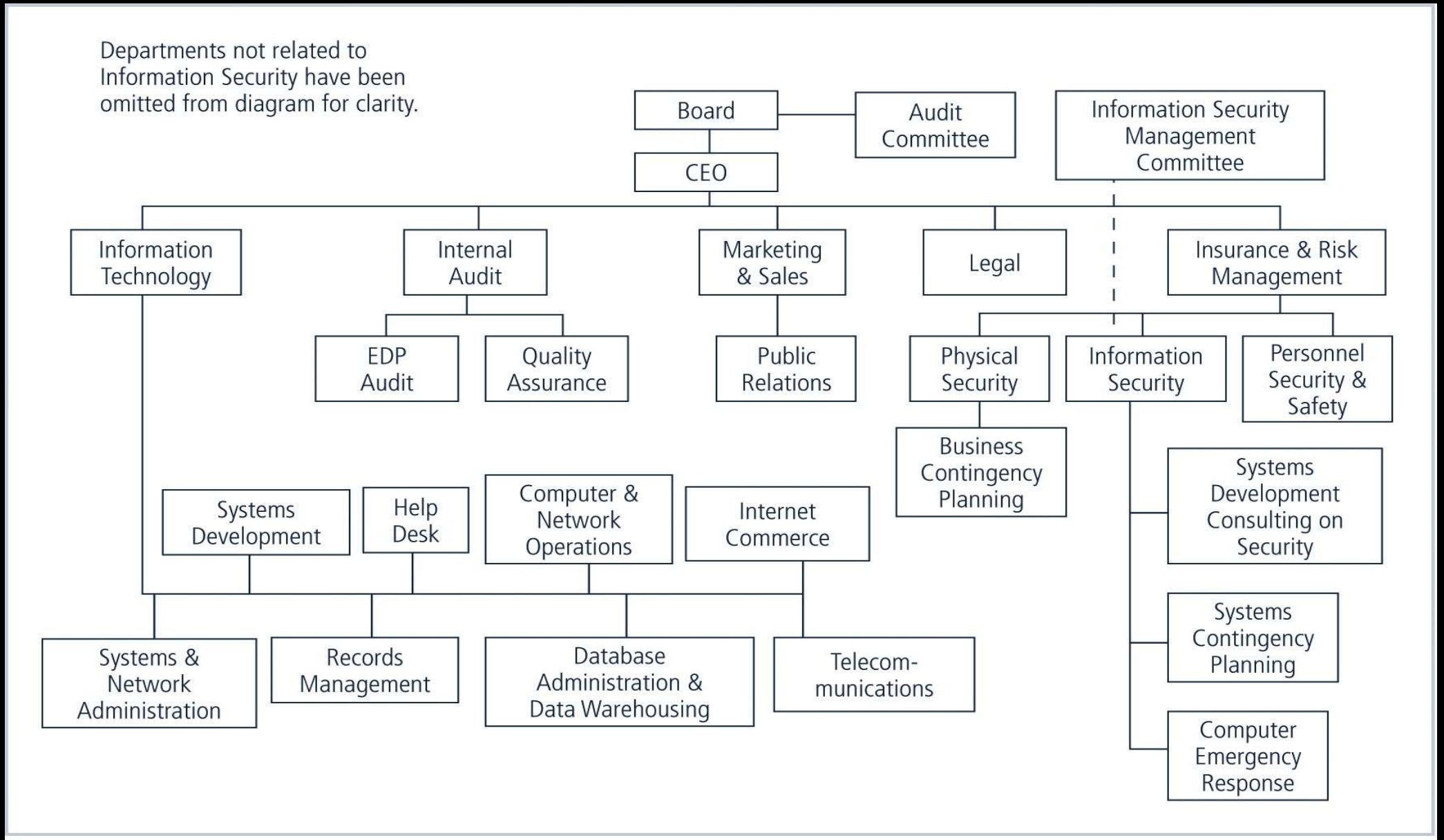
From *Information Security Roles and Responsibilities Made Easy*, used with permission.

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



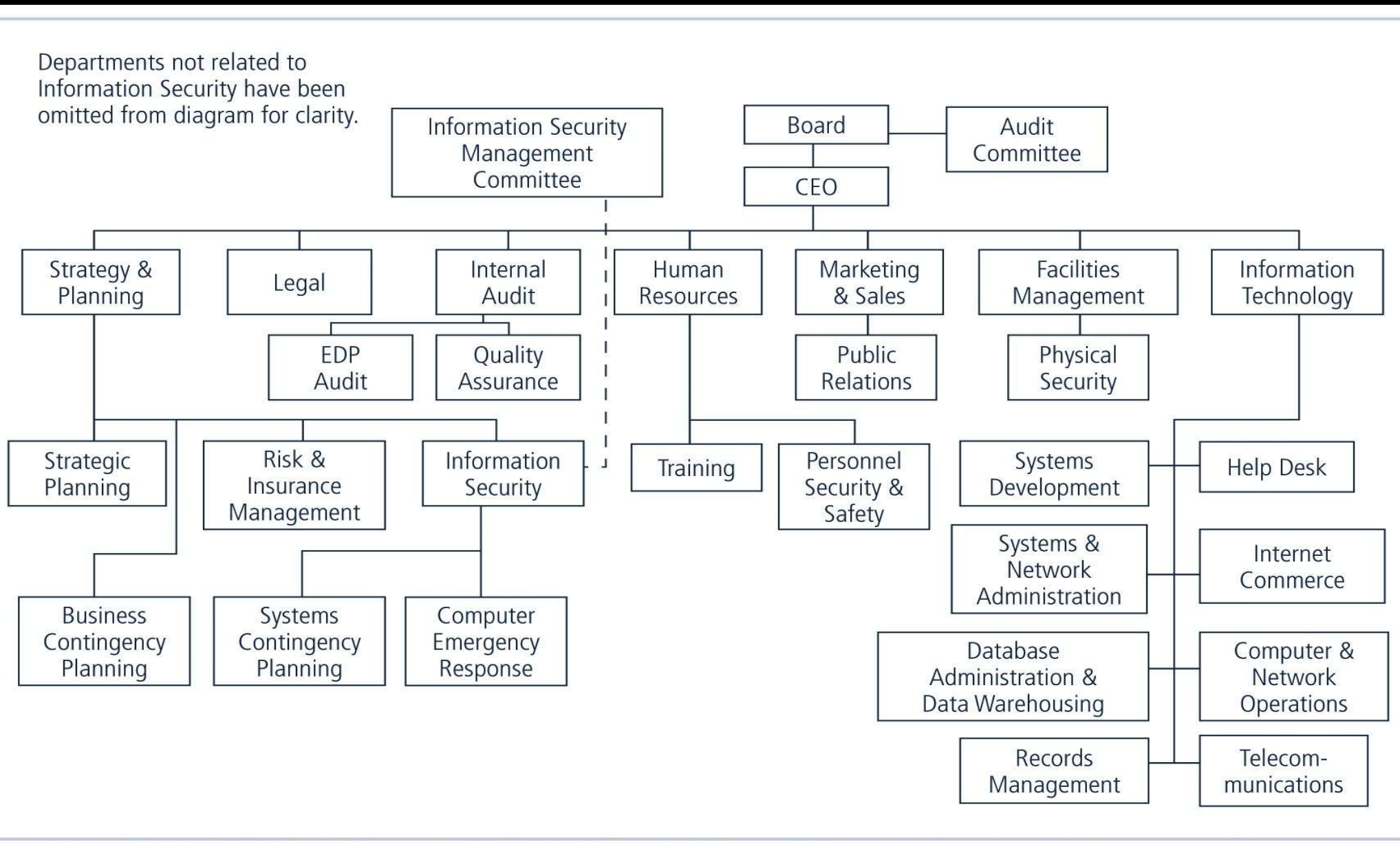
From *Information Security Roles and Responsibilities Made Easy*, used with permission.

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



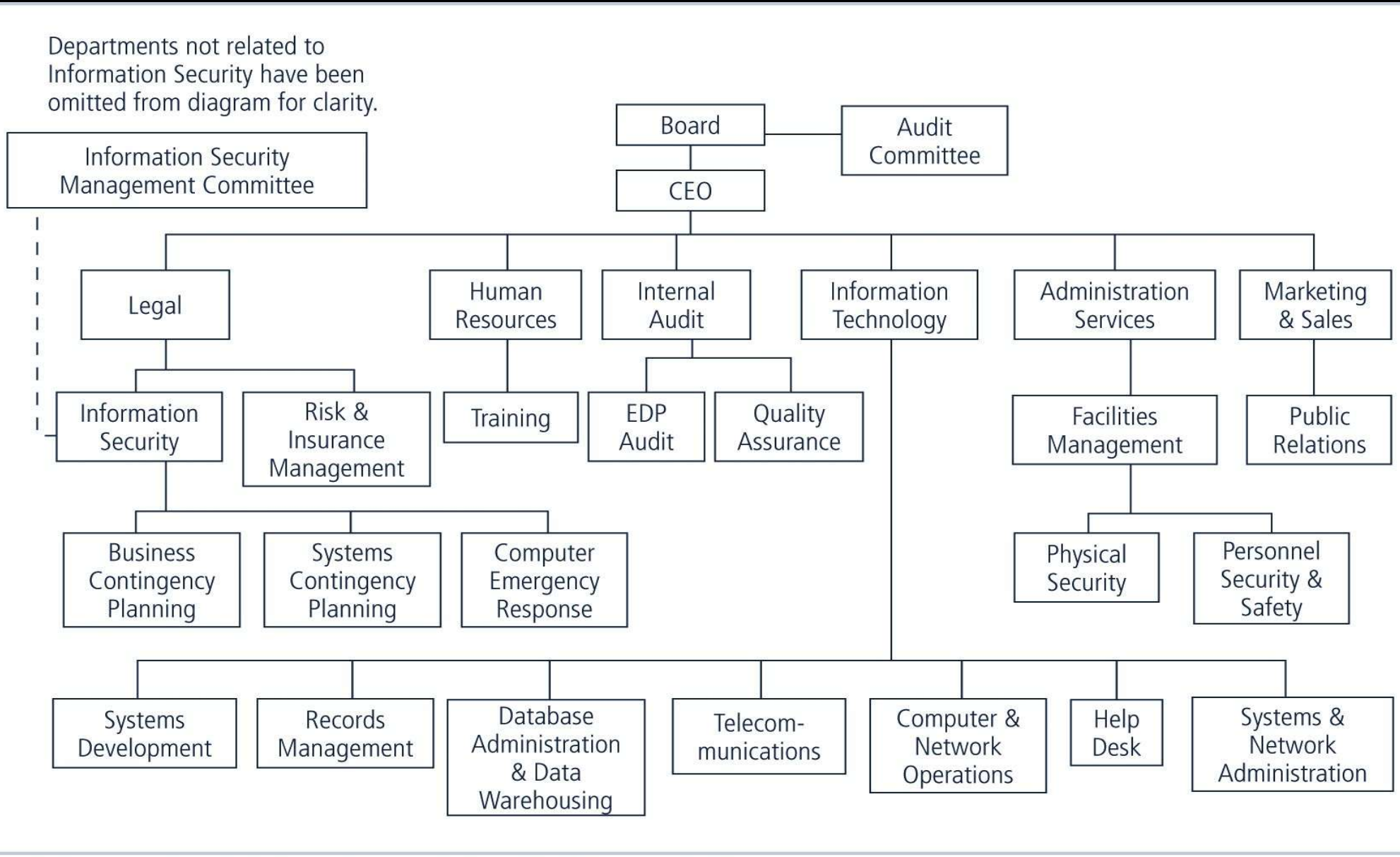
From *Information Security Roles and Responsibilities Made Easy*, used with permission.

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



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.

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

Other options:

Option 7: Internal Audit

Option 8: Help Desk

Option 9: Accounting & Finance Through IT

Option 10: Human Resources

Option 11: Facilities Management

Option 12: Operations

Components of the Security Program

InfoSec needs of any organization
are unique to
the culture, size, & budget
of that organization

Determining what level
the infosec program operates on
depends on the organization's strategic plan;
in particular,
on the plan's vision & mission statements

The CIO & CISO
should use these two documents
to formulate the mission statement
for the infosec program

InfoSec positions can be classified into 1 of 3 types:

1. those that define,
2. those that build, &
3. those that administer

Definers

✓ provide policies, guidelines, & standards
✓ perform consulting & risk assessment
✓ develop product & technical architectures
✓ senior people with a lot of broad knowledge, but often not a lot of depth

Builders

✓ the real techies
✓ create & install security solutions

Administrators

✓ operate & administrate security tools & the security monitoring function
✓ work to continuously improve processes

Typical organization
has a number of individuals
with infosec responsibilities

While the titles used may be different,
most of the job functions
fit into one of the following:

- ✓ Chief infosec Officer (CISO)
- ✓ Security managers
- ✓ Security administrators & analysts
- ✓ Security technicians
- ✓ Security staff

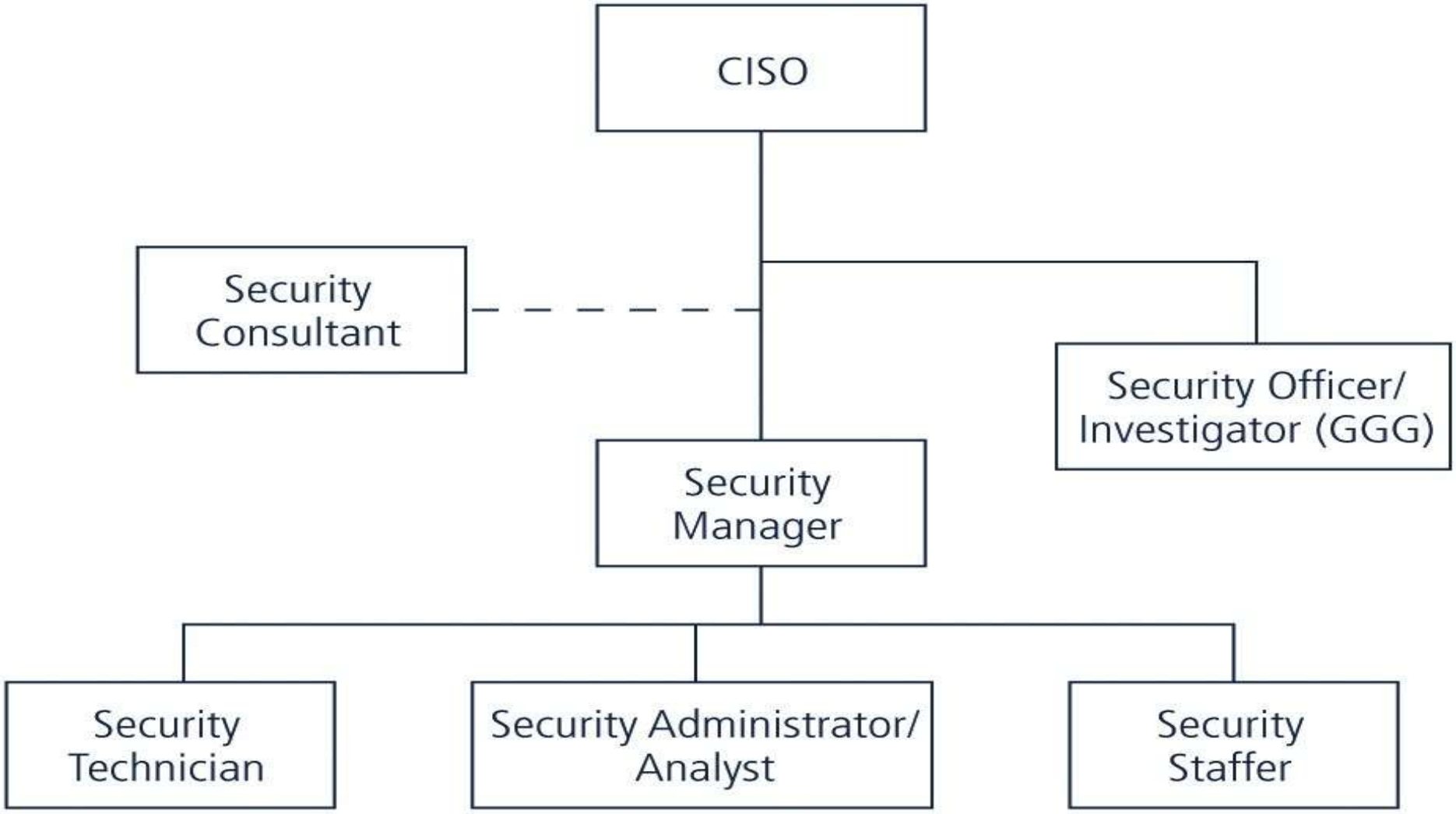


FIGURE 5-11 **Information Security Roles**

Help desk is an important part
of the infosec 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, DOS attack, or a virus

Because help desk technicians
perform a specialized role in infosec,
they have a need for specialized training

Security Education, Training, & Awareness Programs
are designed to reduce
accidental security breaches

Awareness, training, & education programs
offer 2 major benefits:

1. Improve employee behavior

2. Enable organization
to hold employees accountable
for their actions

SETA program consists of three elements:

1. security education

2. security training

3. security awareness

The purpose of SETA
is to enhance security ...

✓ By building in-depth knowledge,
as needed,
to design, implement, or operate
security programs
for organizations & systems

✓ By developing skills & 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 involves
providing detailed information
& hands-on instruction
to give skills to users
to perform their duties securely

Two methods for customizing training

1. Functional background

- ✓ General user
- ✓ Managerial user
- ✓ Technical user

2. Skill level

- ✓ Novice
- ✓ Intermediate
- ✓ Advanced

Using wrong training methods can:

✓ Hinder transfer of knowledge

✓ Lead to unnecessary expense
& frustrated, poorly trained employees

Good training programs:

✓ Use latest learning technologies
& best practices

✓ Recently, less use
of centralized public courses
& 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
& training sessions
that are immediate & consistent,
available during normal work week

Selection of training delivery method
is not always based
on best outcome for the trainee

Other factors,
like budget, scheduling,
& organization’s needs
often come first

Training delivery methods:

- ✓ One-on-One
- ✓ Formal Class
- ✓ Computer-Based Training (CBT)
- ✓ Distance Learning/Web Seminars
- ✓ User Support Group
- ✓ On-the-Job Training
- ✓ Self-Study (Noncomputerized)

Where can you find trainers?

✓ 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

While each organization
develops its own strategy,
the following 7-step methodology
generally applies:

Step 1: Identify program scope, goals, & objectives

Step 2: Identify training staff

Step 3: Identify target audiences

Step 4: Motivate management & employees

Step 5: Administer the program

Step 6: Maintain the program

Step 7: Evaluate the program

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
& 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,
& provide sufficient detail & coverage

✓ Keep things light

more … →

✓ 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 & document all actions

✓ Provide good information early,
rather than perfect information late

10 Commandments of InfoSec Awareness Training

I. InfoSec is a people,
rather than a technical, issue

II. If you want them to understand,
speak their language

III. If they cannot see it, they will not learn it

IV. Make your point so that you can identify it
& so can they

V. Never lose your sense of humor

more ... →

VI. Make your point, support it, & conclude it

VII. Always let the recipients know
how the behavior that you request
will affect them

VIII. Ride the tame horses

IX. Formalize your training methodology

X. Always be timely,
even if it means slipping schedules
to include urgent information

Security awareness & security training
are designed to modify
any employee behavior
that endangers the security
of the organization’s information

Security training & awareness activities
can be undermined, however,
if management
does not set a good example

Effective training & awareness programs
make employees accountable
for their actions

Dissemination & enforcement
of policy become easier
when training & awareness programs
are in place

Demonstrating due care & due diligence
can help indemnify the institution
against lawsuits

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 & frequently changed

Security awareness components
from cheap to very expensive

Security awareness components include:

✓ Videos
✓ Posters & banners
✓ Lectures & conferences
✓ Computer-based training
✓ Newsletters
✓ Brochures & flyers
✓ Trinkets (coffee cups, pens, pencils, T-shirts)
✓ Bulletin boards

Security newsletter is
a cost-effective way
to disseminate security information

In the form of paper, e-mail, or intranet

Goal: keep infosec
uppermost in users' minds
& stimulate them to care about security

Newsletters might include:

✓ Threats to the organization's info assets

✓ Schedules for upcoming security classes & presentations

✓ Addition of new security personnel

✓ Summaries of key policies

✓ Summaries of key news articles

✓ Announcements relevant to infosec

✓ How-to's

Security poster series
can be a simple & 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
& keeping posters updated

✓ Keeping them simple,
but visually interesting

✓ Making the message clear

✓ Providing information
on reporting violations

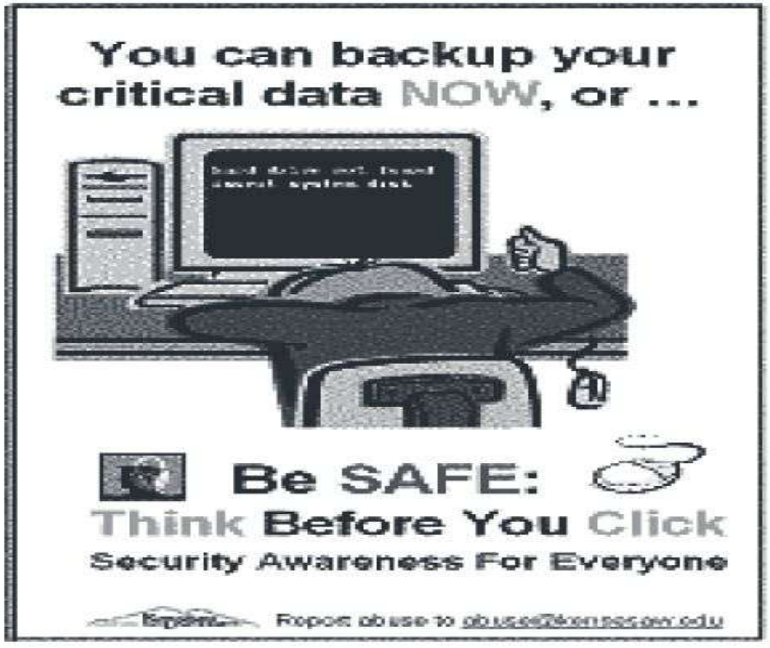


FIGURE 5-15 SETA Awareness Components: Posters

I like some other posters better.

(see www.despair.com)

Trinkets may not
cost much on a per-unit basis,
but they can be expensive
to distribute throughout an organization

Several types of common trinkets:

✓ Pens & pencils
✓ Mouse pads
✓ Coffee mugs
✓ Plastic cups
✓ Hats
✓ T-shirts

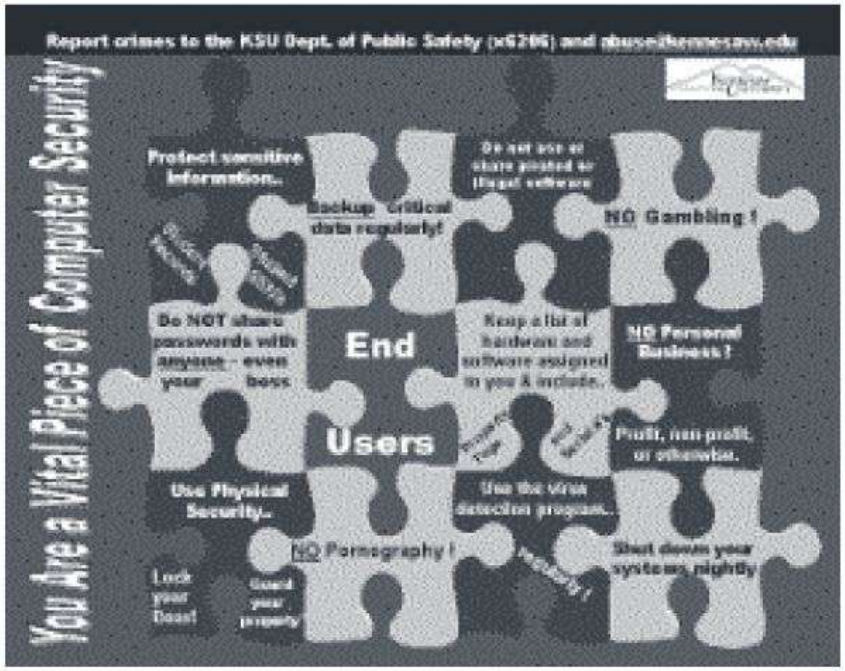


FIGURE 5-16 SETA Awareness Components: Trinkets

Organizations can establish
Web pages or sites
dedicated to
promoting infosec awareness

As with other SETA awareness methods,
the challenge lies
in updating the messages
frequently enough
to keep them fresh

Some tips on creating & maintaining an educational Web site:

✓ See what’s already out there

✓ Plan ahead

✓ Keep page loading time to a minimum

✓ Seek feedback

✓ Assume nothing & check everything

✓ Spend time promoting your site

Another means
of renewing the infosec message
is to have a guest speaker
or even a mini-conference
dedicated to the topic of infosec

Perhaps in association with
National Computer Security Day:
November 30

Summary

Organizing for Security

Placing InfoSec Within An Organization

Components of the Security Program

InfoSec Roles & Titles

Implementing Security
Education, Training, & Awareness Programs

Thank you!

Scott Granneman