QUẢN LÝ AN TOÀN THÔNG TIN

BÀI 5: PHÁT TRIỂN CHƯƠNG TRÌNH ĐẢM BẢO AN TOÀN THÔNG TIN

Nguyên tắc quản lý ATTT

Các đặc điểm sau sẽ là trọng tâm của khóa học hiện tại (sáu chữ P):

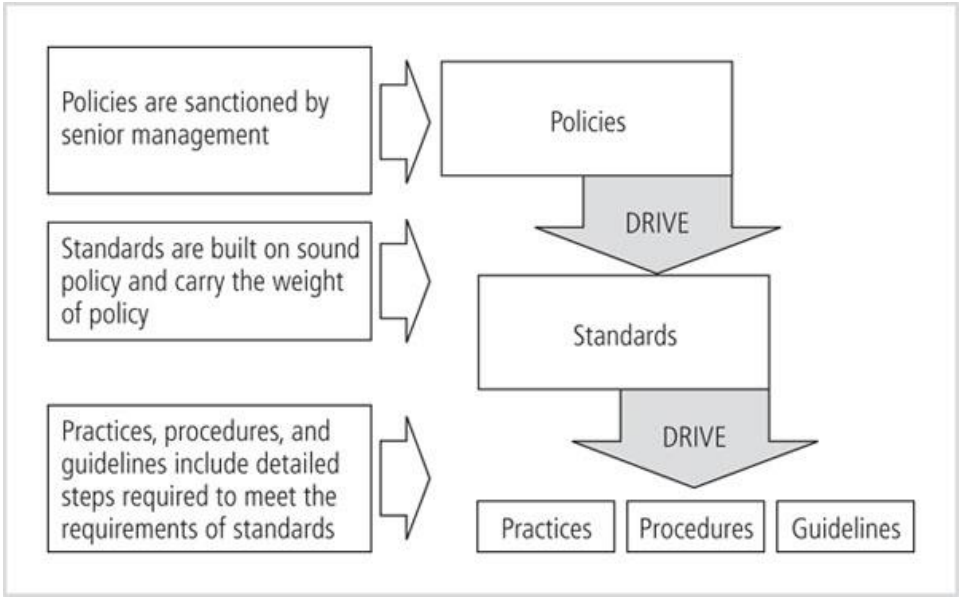
1. Lập kế hoạch
2. Chính sách
3. Các chương trình
4. Sự bảo vệ
5. Con người
6. Quản lý dự án

http://csrc.nist.gov/publications/PubsTC.html

1. CHÍNH SÁCH, TIÊU CHUẨN VÀ THÔNG LỆ

- ***Chính sách:***

  Chính sách được phê chuẩn bởi các quản lý cấp cao. Gồm 3 loại chính sách: Chính sách cho doanh nghiệp; Chính sách cho các vấn đề cụ thể và Chính sách cho hệ thống cụ thể.



- ***Tiêu chuẩn:***

  Các tiêu chuẩn dựa trên chính sách đúng đắn

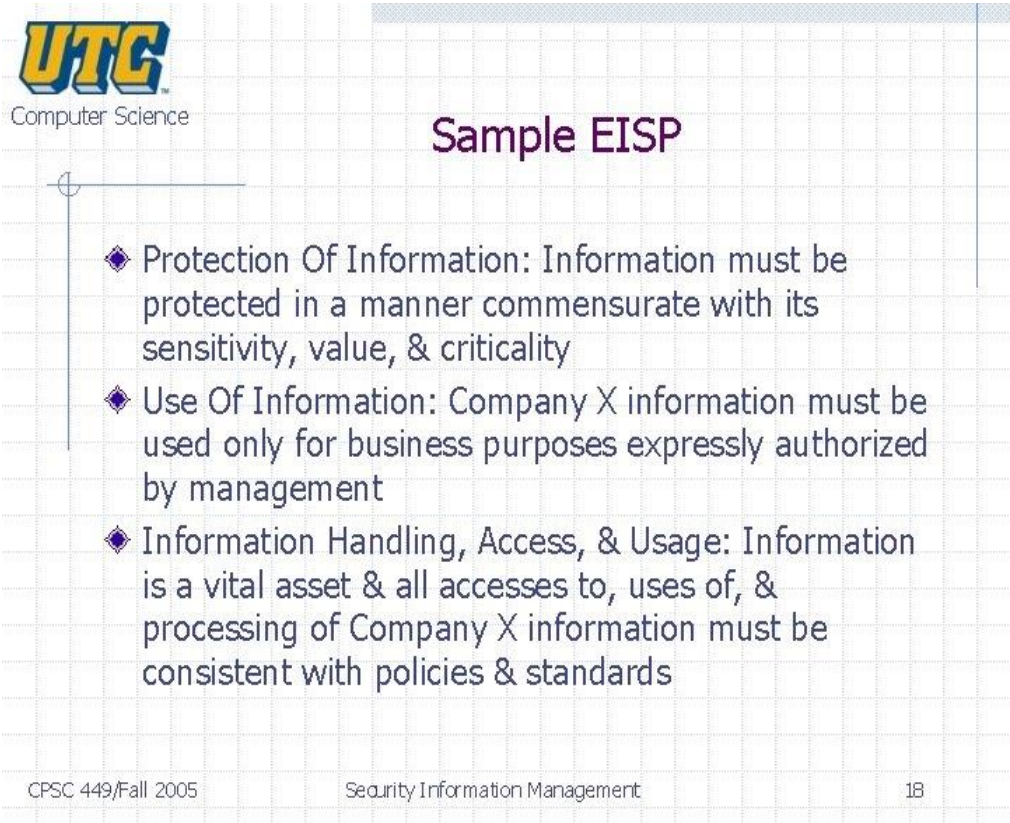
- ***Thông lệ:***

  Các thông lệ, thủ tục và các hướng dẫn bao gồm chi tiết các bước được yêu cầu để đáp ứng các nhu cầu của tiêu chuẩn

1. CHÍNH SÁCH, TIÊU CHUẨN VÀ THÔNG LỆ

1.1 Chính sách an toàn cho công ty (EISP)

- Định hướng chiến lược, phạm vi và sứ mệnh cho các nỗ lực bảo mật của tổ chức.
- Giao phó trách nghiệm cho các lĩnh vực an toàn thông tin khác nhau.



1. CHÍNH SÁCH, TIÊU CHUẨN VÀ THÔNG LỆ

1.2 Chính sách an toàn cho các vấn đề cụ thể (ISSP)

- Cung cấp hướng dẫn chi tiết các mục tiêu
- Bảo vệ tổ chức khỏi sự kém hiệu quả và mơ hồ
- Bồi thường cho tổ chức chịu trách nhiệm pháp lý đối với việc sử dụng hệ thống bất hợp pháp

1. CHÍNH SÁCH, TIÊU CHUẨN VÀ THÔNG LỆ

1.3 Chính sách an toàn cho các hệ thống cụ thể (SysSP)

- Các chính sách bảo mật dành riêng cho hệ thống (SysSP) thường không giống các loại chính sách khác.
- Chính sách bảo mật dành riêng cho hệ thống gồm:
  - Hướng dẫn quản lý
  - Thông số kỹ thuật

1. CHÍNH SÁCH, TIÊU CHUẨN VÀ THÔNG LỆ

1.4 Nguyên tắc cho chính sách hiệu quả

Để các chính sách có hiệu quả, chúng phải đáp ứng:

- Đã được phát triển
- Đã được phân phối hoặc phổ biến
- Đã đánh giá
- Đã được hiểu
- Đã được phải chính thức đồng ý
- Đã được áp dụng và thực thi thống nhất

2. GIỚI THIỆU VỀ CHƯƠNG TRÌNH ĐẢM BẢO ATTT

2.1 Tổ chức an ninh

- Chương trình đảm bảo an toàn thông tin được sử dụng để mô tả cấu trúc và nỗ lực phòng chống rủi ro đối với tài sản thông tin của tổ chức.

2. GIỚI THIỆU VỀ CHƯƠNG TRÌNH ĐẢM BẢO ATTT

2.1 Tổ chức an ninh

- Có rất nhiều thứ ảnh hưởng đến việc xây dựng chương trình đảm bảo ATTT:
  - Văn hóa
  - Ngân sách
  - Quy mô công ty: khi một công ty phát triển quy mô, bộ phận an ninh sẽ không theo kịp những cơ sở hạ tầng phức tạp

Quản lý cấp cao sẽ có 1 cái nhìn tích cực hay tiêu cực về chương trình bảo mật

→ Ảnh hưởng tới việc hỗ trợ, duy trì và mở rộng của chương trình bảo mật về nhiều mặt (nhân lực, ngân sách, …)

Ngân sách

- Gồm: ngân sách nhân sự, ngân sách vốn và chi phí
- Ngân sách của chương trình bảo mật phải phù hợp với tổng ngân sách của tổ chức.

- Các tổ chức càng lớn thì chương trình bảo mật càng lớn và ngược lại.
- Quy mô của tổ chức càng tăng, bộ phận bảo mật không theo kịp cơ sở hạ tầng ngày càng phức tạp của tổ chức.

2. GIỚI THIỆU VỀ CHƯƠNG TRÌNH ĐẢM BẢO ATTT

2.1 Tổ chức an ninh

Doanh nghiệp lớn:

- Trưởng phòng ATTT chịu trách nhiệm về các chức năng bảo mật thông tin.
- Việc triển khai nhân viên an ninh toàn thời gian phụ thuộc vào:
  - Độ nhạy cảm của thông tin cần bảo vệ
  - Quy định của ngành
  - Lợi nhuận chung
  - Ràng buộc ngân sách

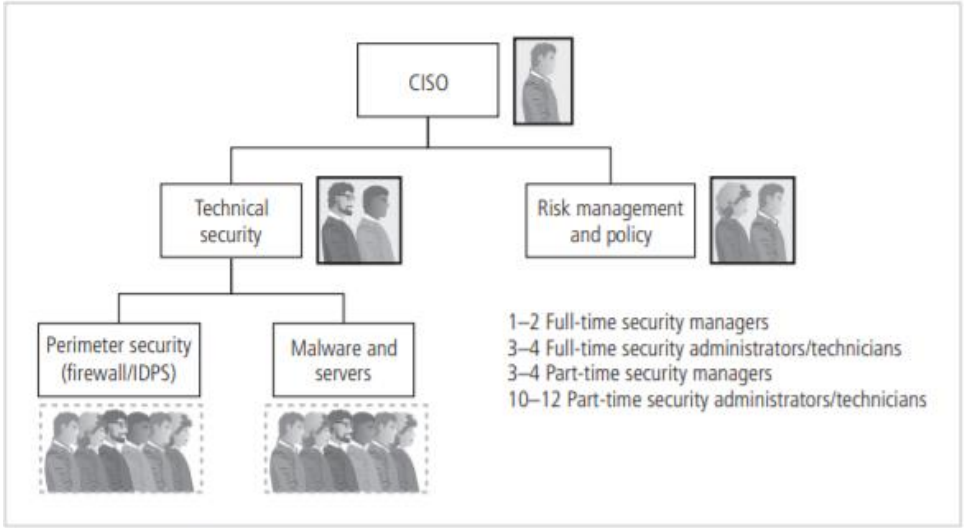


Figure 5-1 Example of InfoSec staffing in a large organization

2. GIỚI THIỆU VỀ CHƯƠNG TRÌNH ĐẢM BẢO ATTT

2.1 Tổ chức an ninh

Doanh nghiệp lớn:

- Ngân sách cho bảo mật chiếm khoảng 5% tổng ngân sách IT
- Phương pháp tiếp cận bảo mật hợp lý hơn, kết hợp kế hoạch và chính sách vào văn hóa doanh nghiệp.
- 1 cách tiếp cận phân tách chức năng thành 4 lĩnh vực:
  - Đơn vị phi kỹ thuật ngoài lĩnh vực IT: pháp lý, đào tạo
  - Các nhóm IT ngoài lĩnh vực bảo mật thông tin: quản trị an ninh mạng,
  - Bảo mật thông tin có chiều sâu (dịch vụ khách hàng): đo lường, lập kế hoạch,..
  - Bảo mật thông tin có chiều sâu (bắt buộc): chính sách, kiểm toán, …

Các chức năng về ATTT trong tổ chức có quy mô lớn

Chức năng	Mô tả	Comments
Risk assessment (Đánh giá rủi ro)	Xác định và đánh giá rủi ro hiện diện trong các sáng kiến hoặc hệ thống IT	Chức năng này bao gồm việc xác định các nguồn rủi ro và có thể bao gồm việc đưa ra lời khuyên về các biện pháp kiểm soát có thể làm giảm rủi ro.
Risk management (Quản lý rủi ro)	Thực hiện hoặc giám sát việc sử dụng các biện pháp kiểm soát để giảm rủi ro	Chức năng này thường được kết hợp với đánh giá rủi ro.
Systems testing (Kiểm thử hệ thống)	Đánh giá các bản vá được sử dụng để đóng các lỗ hổng phần mềm và kiểm thử chấp nhận các hệ thống mới để đảm bảo tuân thủ chính sách và hiệu quả	Chức năng này thường là một phần của các chức năng ứng phó sự cố hoặc quản lý rủi ro.
Policy (Chính sách)	Duy trì và thúc đẩy chính sách InfoSec trong toàn bộ tổ chức	Chức năng này phải được phối hợp với các chính sách của tổ chức
Legal assessment (Đánh giá pháp lý)	Duy trì nhận thức về các luật được dự định và thực tế cũng như tác động của chúng, đồng thời phối hợp với các cố vấn pháp lý và cơ quan thực thi pháp luật bên ngoài	Chức năng này hầu như luôn ngoài lề đối với bộ phận InfoSec và CNTT.
Planning (Lập kế hoạch)	Nghiên cứu, tạo, duy trì và thúc đẩy các kế hoạch InfoSec; thường áp dụng cách tiếp cận quản lý dự án để lập kế hoạch trái ngược với kế hoạch chiến lược cho toàn tổ chức	Chức năng này phải phối hợp với các quy trình chính sách trong toàn tổ chức
Measurement (Đo lường)	Sử dụng các hệ thống điều khiển hiện có (hệ thống thu thập dữ liệu chuyên dụng) để đo lường tất cả các khía cạnh của InfoSec	Quản lý dựa vào các số liệu thống kê kịp thời và chính xác đã dựa vào để đưa ra các quyết định sáng suốt.
Compliance	Xác minh rằng quản trị viên hệ thống và mạng sửa chữa kịp thời và chính xác các lỗ hổng được xác định	Chức năng này đặt ra các vấn đề đối với dịch vụ khách hàng tốt vì rất khó để khách hàng tập trung và thực thi tuân thủ cùng một lúc.
Centralized authentication (Xác thực tập trung)	Quản lý việc cấp và thu hồi thông tin đăng nhập mạng và hệ thống cho tất cả các thành viên của tổ chức	Chức năng này thường được giao cho bộ phận trợ giúp hoặc nhân viên kết nối với chức năng bộ phận trợ giúp
Systems security administration (Quản trị viên bảo mật hệ thống)	Quản lý cấu hình của hệ thống máy tính, thường được sắp xếp thành nhóm theo hệ điều hành mà chúng chạy	Nhiều tổ chức có thể đã chỉ định một số chức năng bảo mật ban đầu cho các nhóm này bên ngoài chức năng InfoSec. Đây có thể là một nguồn xung đột khi các tổ chức cập nhật các chương trình InfoSec.

2. GIỚI THIỆU VỀ CHƯƠNG TRÌNH ĐẢM BẢO ATTT

2.1 Tổ chức an ninh

Doanh nghiệp trung bình:

- Ngân sách bảo mật chiếm khoảng 11% tổng ngân sách IT
- Có xu hướng bỏ qua một số chức năng bảo mật.
- Tuy nhiên vẫn có thể có quy mô đủ lớn để triển khai phương pháp bảo mật nhiều tầng.

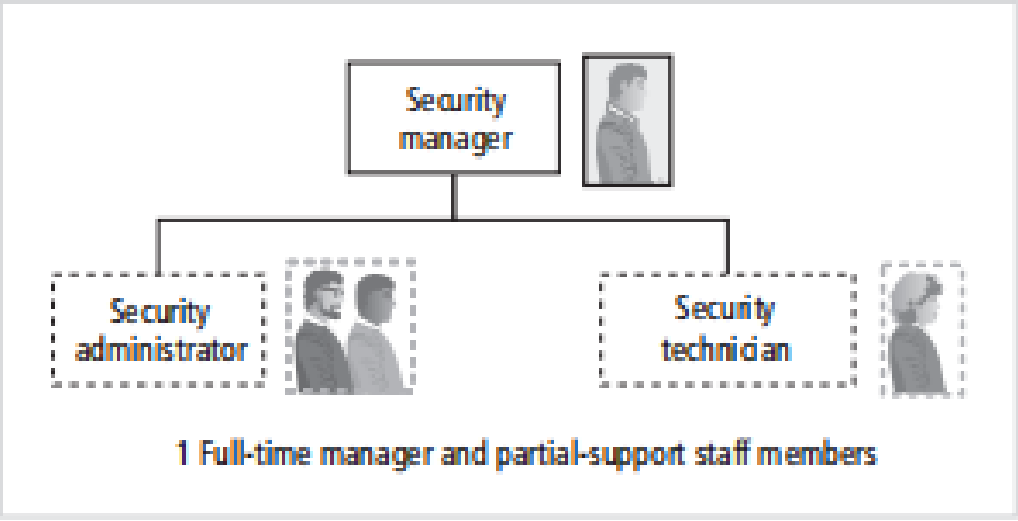


Figure 5-3 Example of InfoSec staffing in a medium-sized organization

2. GIỚI THIỆU VỀ CHƯƠNG TRÌNH ĐẢM BẢO ATTT

2.1 Tổ chức an ninh

Doanh nghiệp nhỏ:

- Mô hình tổ chức đơn giản, thường tập trung vào CNTT.
- Ngân sách không cân xứng cho bảo mật.
- Các chính sách về ATTT mang tính hình thức
- Thường thuê các chức năng từ bên ngoài.
- Mối đe doạ từ nội bộ công ty ít hơn do các nhân viên đều biết nhau.

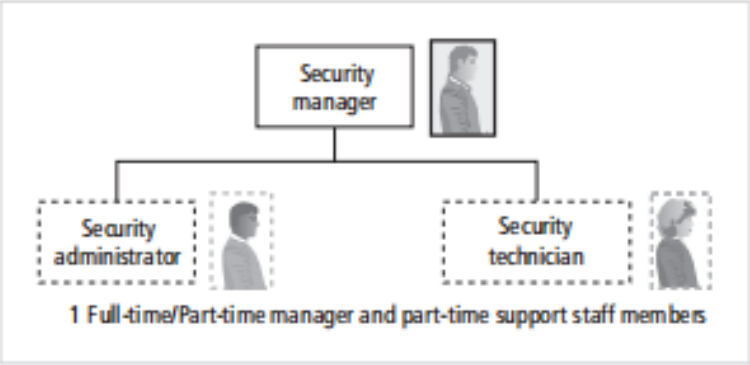


Figure 5-4 Example of InfoSec staffing in a smaller organization

Đưa an toàn thông tin trong một tổ chức

Trong các tổ chức lớn, bộ phận bảo mật thường nằm trong bộ phận CNTT đứng đầu bởi CISO người báo cáo trực tiếp cho CIO.

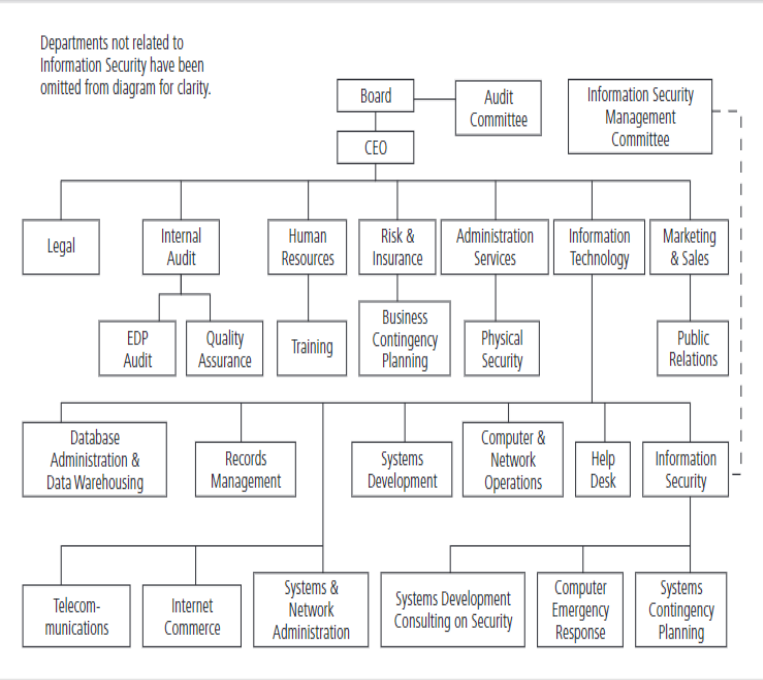
- Trong thực tế, điều này không phải luôn như vậy. Bởi về bản chất, một chương trình bảo mật thông tin hoạt động đôi khi có thể gây mâu thuẫn với mục tiêu ngắn hạn hoặc lâu dài của bộ phận IT lớn hơn.

- Các tổ chức thường chọn ra quản lý cấp trung đóng vai trò gửi các báo cáo cho Giám đốc điều hành. Họ thường có những đặc điểm:

- Luôn chào đón tiếp nhận ý tưởng mới
- Có ảnh hưởng với ban lãnh đạo
- Được nhân viên tôn trọng
- Quen thuộc và hiểu rõ các khái niệm hệ thống thông tin cơ bản.
- Luôn giữ vững lập trường
- Có tầm nhìn về tương lai IT và quan tâm cao đến bảo mật

Các mô hình báo cáo mà các tổ chức thường dùng

Option 1: IT



- CISO báo cáo tới CIO và CIO báo cáo tới CEO
- Báo cáo của CIO tới CEO sẽ ảnh hưởng tới CISO

❑ **Ưu điểm:**

✓ Chỉ có 1 quản lí trung gian giữa CISO và CEO là CIO - người có kiến thức về IT

✓ Thuận tiện do nhân viên phòng bảo mật thông tin hằng ngày phải dành nhiều thời gian với nhân viên phòng IT.

❑ **Nhược điểm:**

✓ Xung đột lợi ích giữa CISO và CIO

✓ Kết luận ngụ ý rằng bảo mật thông tin hoàn toàn là một vấn đề về công nghệ

Các mô hình báo cáo mà các tổ chức thường dùng

Option 1: IT

- CISO báo cáo tới CIO và CIO báo cáo tới CEO

hưởng tới CISO

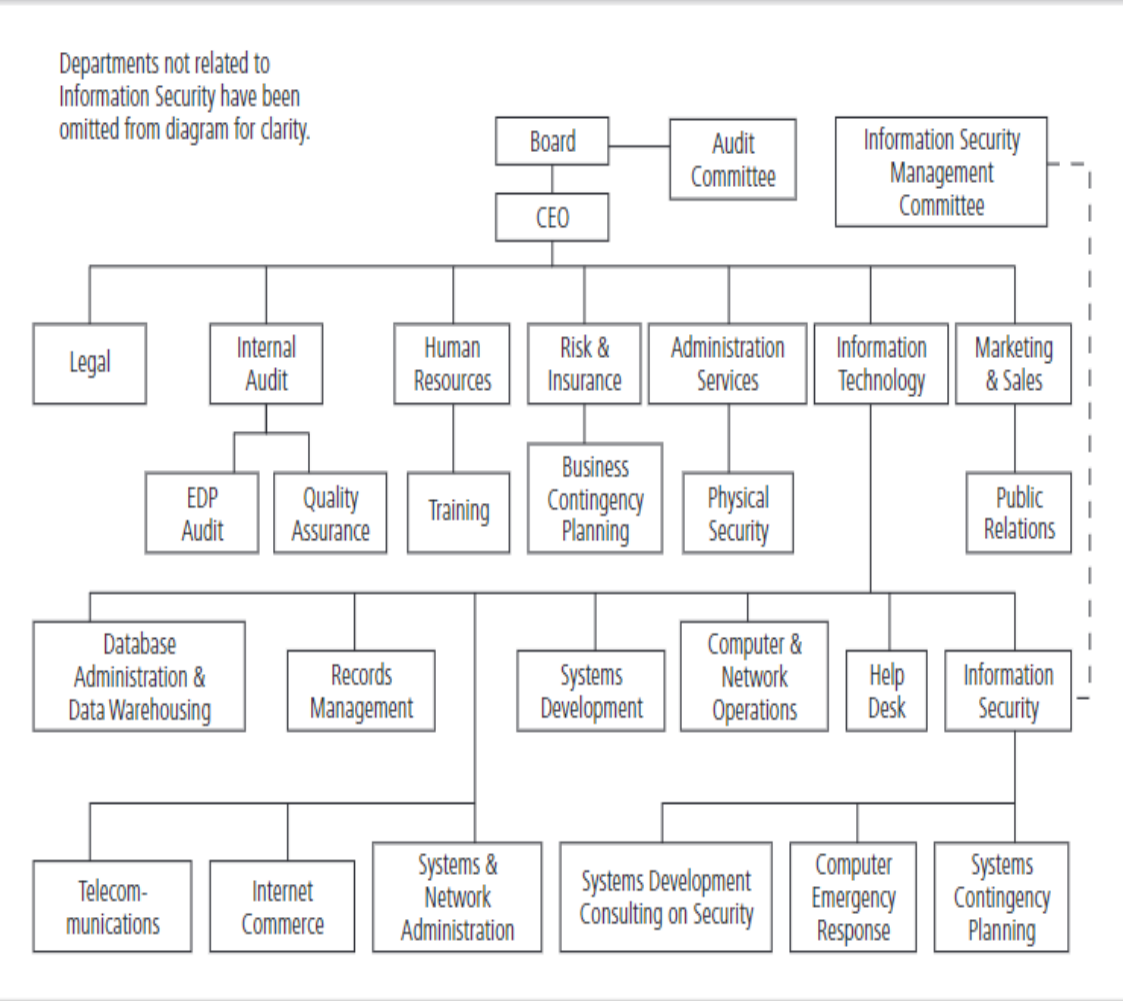
a CISO và CEO là

bảo mật thông tin

gian với nhân

CIO

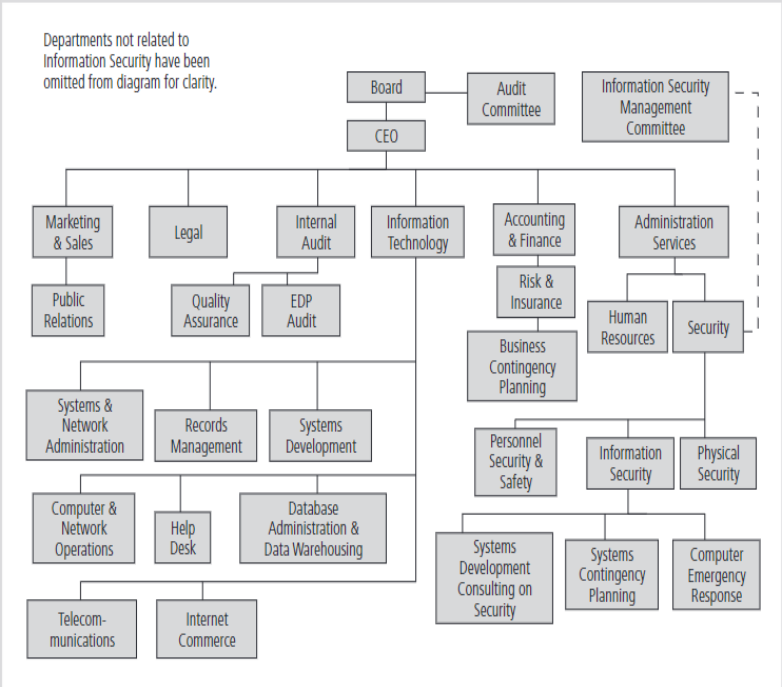
ông tin hoàn toàn là



Các mô hình báo cáo mà các tổ chức thường dùng

Option 2: Bảo mật (Security)

- Phòng bảo mật thông tin báo cáo tới phòng bảo mật



❑ **Ưu điểm:**

✓ Tạo điều kiện trao đổi giữa những người có quan điểm và trách nhiệm liên quan đến bảo mật

✓ Mang lại quan điểm bảo vệ lâu dài đối với các hoạt động bảo mật thông tin

✓ Giảm chi phí của hệ thống bảo mật thông tin

❑ **Nhược điểm:**

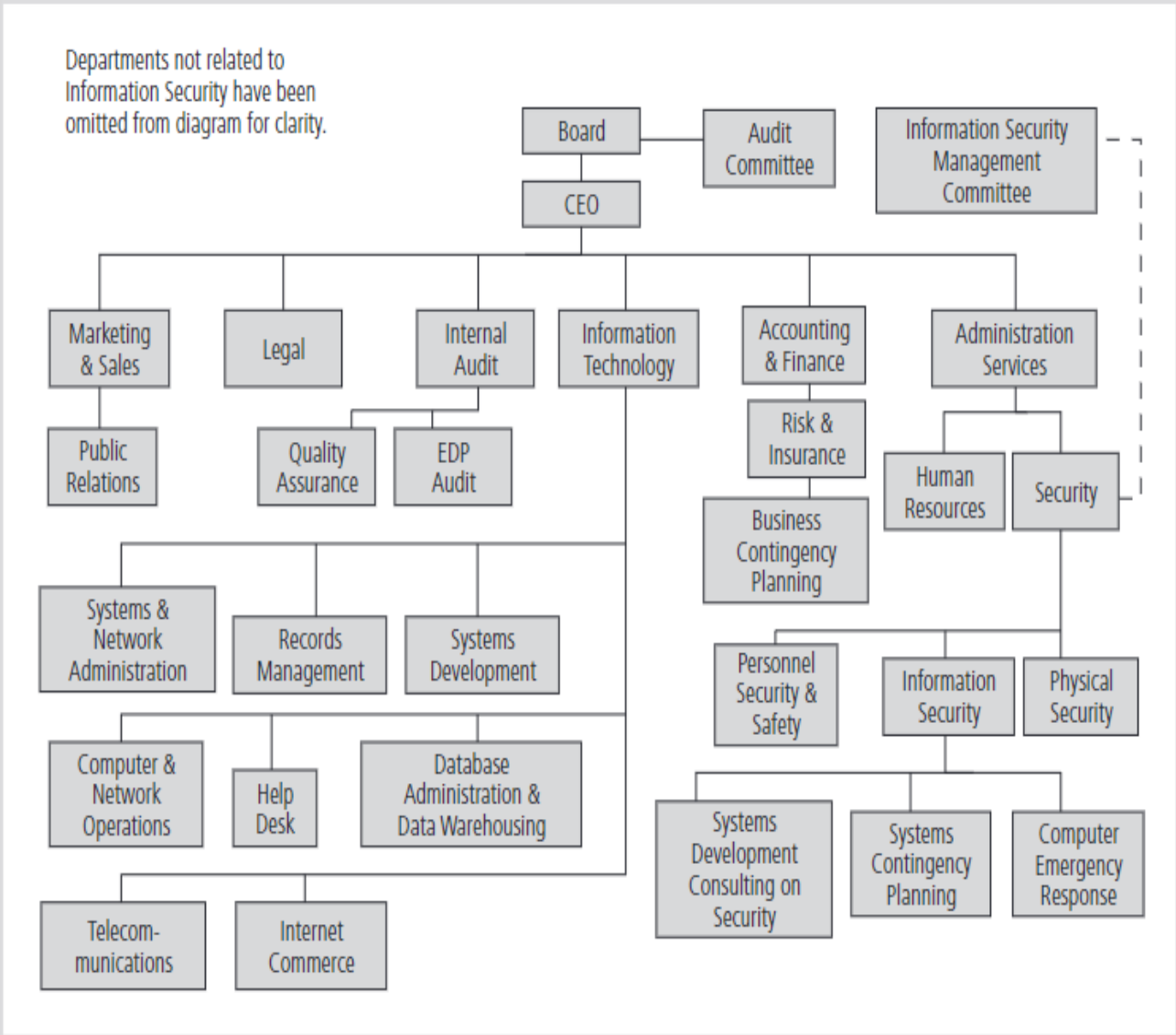
✓ Sự khác biệt giữa bảo mật thông tin và bảo mật vật lí

✓ Phải báo cáo qua 2 lớp trung gian mới đến được với CEO

✓ Quản lý phòng bảo mật có thể thiếu những đánh giá cao về vấn đề bảo mật thông tin với các quản lý cấp cao

Các mô hình báo cáo mà các tổ chức thường dùng

Option 2: Bảo mật (Security) - Phòng bảo mật thông tin báo cáo tới phòng bảo mật



ửng
hiệm liên

dài đối với
n
mật thông tin

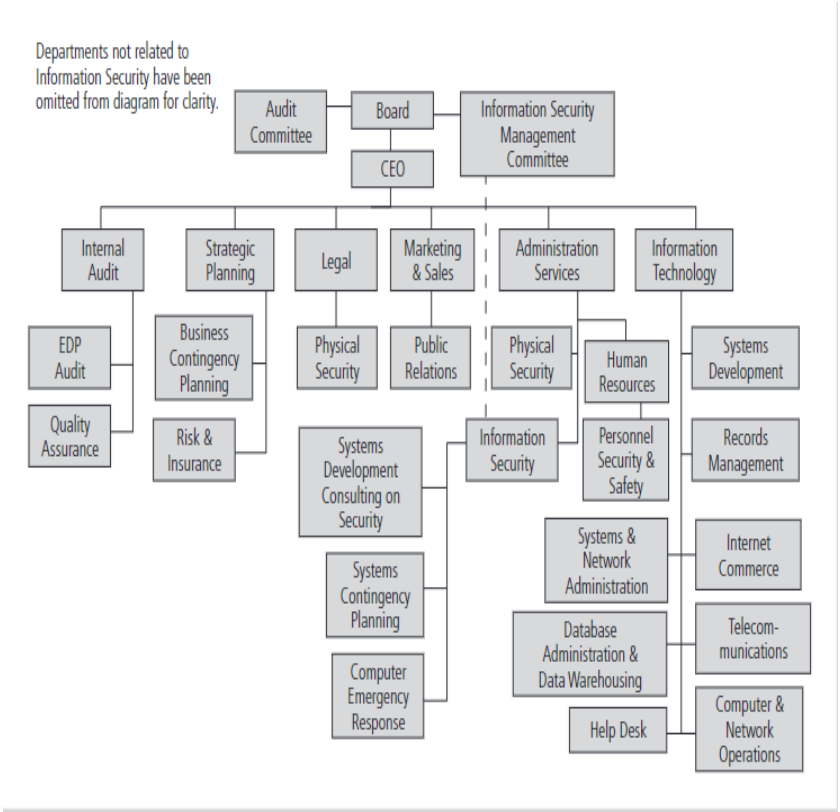
g tin và bảo

ian mới đến

thiếu những
t thông tin với

Các mô hình báo cáo mà các tổ chức thường dùng

Option 3: Dịch vụ quản lý



- CISO báo cáo tới quản lý phòng hỗ trợ quản lý hoặc tới phó chủ tịch quản lý

❑ **Ưu điểm:**

✓ Chỉ có 1 quản lí trung gian giữa CISO và CEO

✓ Thông tin, hệ thống thông tin, nhân viên trong tổ chức đều phải làm việc với phòng bảo mật thông tin

✓ Hỗ trợ bảo mật thông tin dưới mọi hình thức: giấy tờ, lời nói,…

❑ **Nhược điểm:**

✓ Có thể gây cản việc trao đổi với CEO về bảo mật thông tin do phòng hỗ trợ quản lý có thể không biết nhiều về hệ thống IT.

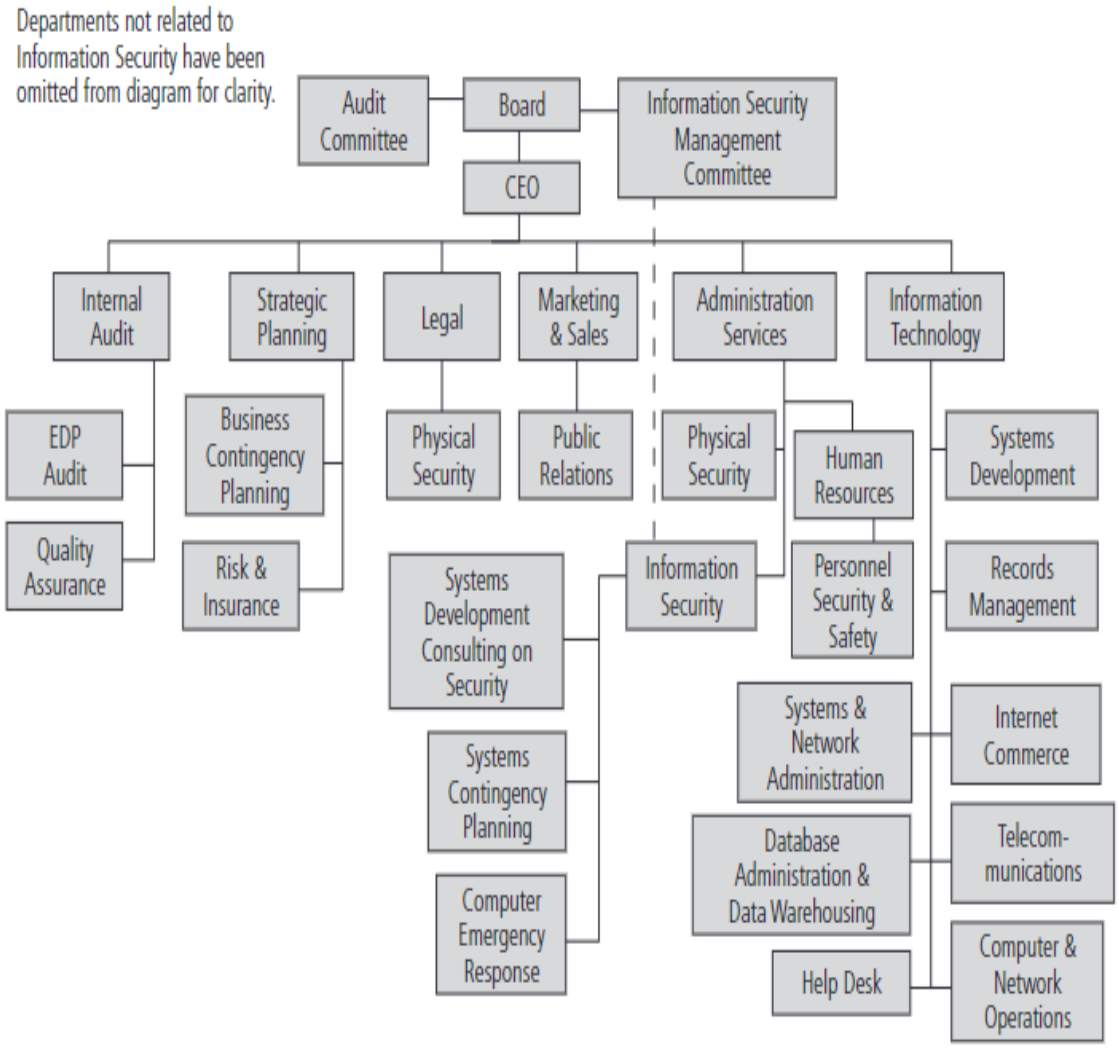
✓ Có thể phải chịu áp lực cắt giảm nhiều chi phí từ quản lý cấp cao

➢ Được đề xuất cho các tổ chức không chuyên sâu về bảo mật thông tin (VD: chuỗi nhà hàng, ...)

Các mô hình báo cáo mà các tổ chức thường dùng

Option 3: Dịch vụ quản lý

- CISO báo cáo tới quản lý phòng hỗ trợ quản lý



ữa CISO và CEO

n, nhân viên
việc với phòng

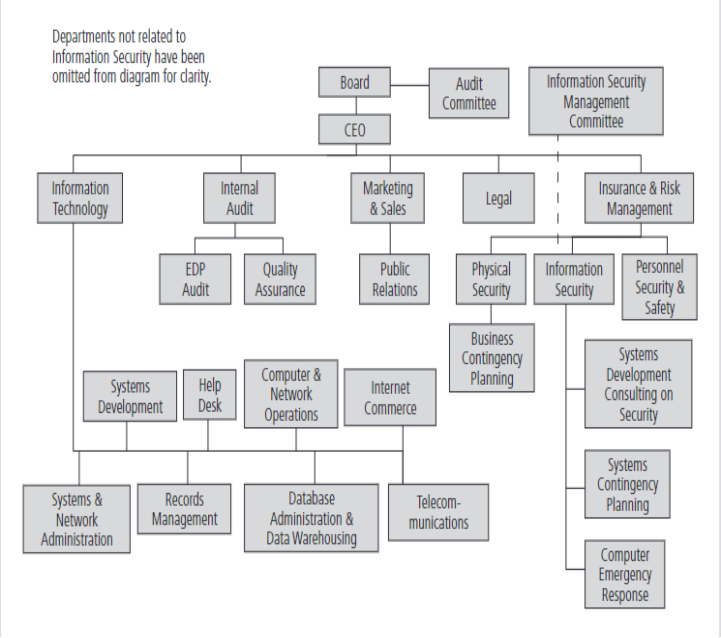
ới mọi hình

với CEO về bảo
rợ quản lý có thể
g IT.
iảm nhiều chi

c không chuyên
): chuỗi nhà

Các mô hình báo cáo mà các tổ chức thường dùng

Option 4: Quản lí rủi ro và bảo hiểm



- CISO báo cáo giám đốc quản lý rủi ro (CRM) hoặc phó chủ tịch quản lý rủi ro và bảo hiểm

❑ **Ưu điểm:**

✓ Tập trung ưu tiên và so sánh tất cả rủi ro trong toàn bộ tổ chức để đánh giá tổn thất tiềm ẩn trên tất cả các bộ phận chức năng của tổ chức

✓ Chỉ có 1 quản lý trung gian giữa CISO và CEO

✓ Phòng ngừa có định hướng và được áp dụng dài hạn

✓ CRM thu hút CEO tham gia vào cuộc thảo luận chấp nhận rủi ro, giảm thiểu rủi ro và chuyển rủi ro.

❑ **Nhược điểm:**

✓ CRM thường không quen thuộc với hệ thống IT

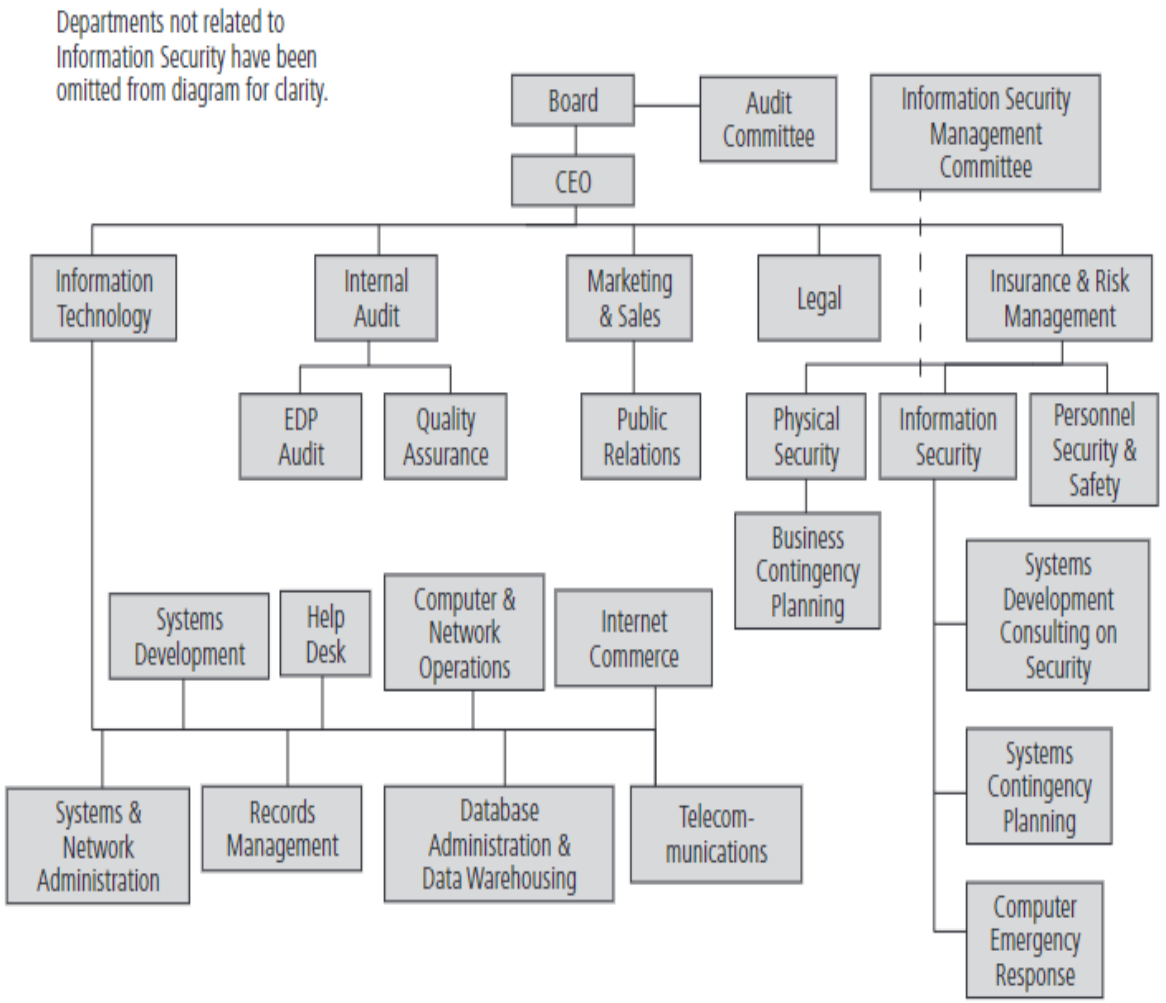
✓ Trọng tâm chiến lược, các khía cạnh vận hành và quản trị của bảo mật thông tin có thể không nhận được sự quan tâm xứng đáng từ CRM.

➢ Đề xuất cho những tổ chức cần chuyên sâu về bảo mật thông tin (VD: ngân hàng, viện nghiên cứu,..)

Các mô hình báo cáo mà các tổ chức thường dùng

Option 4: Quản lí rủi ro và bảo hiểm

- CISO báo cáo giám đốc quản lý rủi ro (CRM) hoặc phó



g toàn bộ
à các bộ

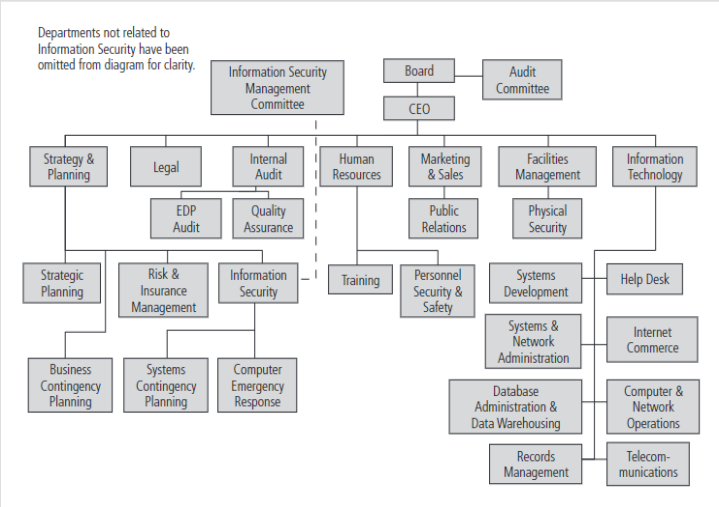
O
lài hạn
àn chấp
.

IT
à và quản
ược sự

bảo mật

Các mô hình báo cáo mà các tổ chức thường dùng

Option 5: Chiến lược và kế hoạch



- Quản lý phòng an toàn thông tin báo cáo tới phó chủ tịch chiến lược và kế hoạch
- Xem chức năng bảo mật thông tin là quan trọng đối với thành công của tổ chức

❑ **Ưu điểm:**

✓ Chỉ có 1 quản lý trung gian giữa CISO và CEO

✓ Nhấn mạnh nhu cầu về các yêu cầu bảo mật thông tin dạng văn bản (chính sách, tiêu chuẩn, thủ tục, ...)

✓ Truyền đạt rằng InfoSec là vấn đề quản lý và con người, không chỉ là vấn đề công nghệ

❑ **Nhược điểm:**

✓ Trọng tâm là chiến lược và các khía cạnh hoạt động và quản trị của an ninh thông tin có thể không được phó chủ tịch chiến lược và kế hoạch chú ý

➢ Đề xuất cho những tổ chức kinh doanh trên Internet hoặc các công ty thẻ tín dụng.

Các mô hình báo cáo mà các tổ chức thường dùng

Option 5: Chiến lược và kế hoạch

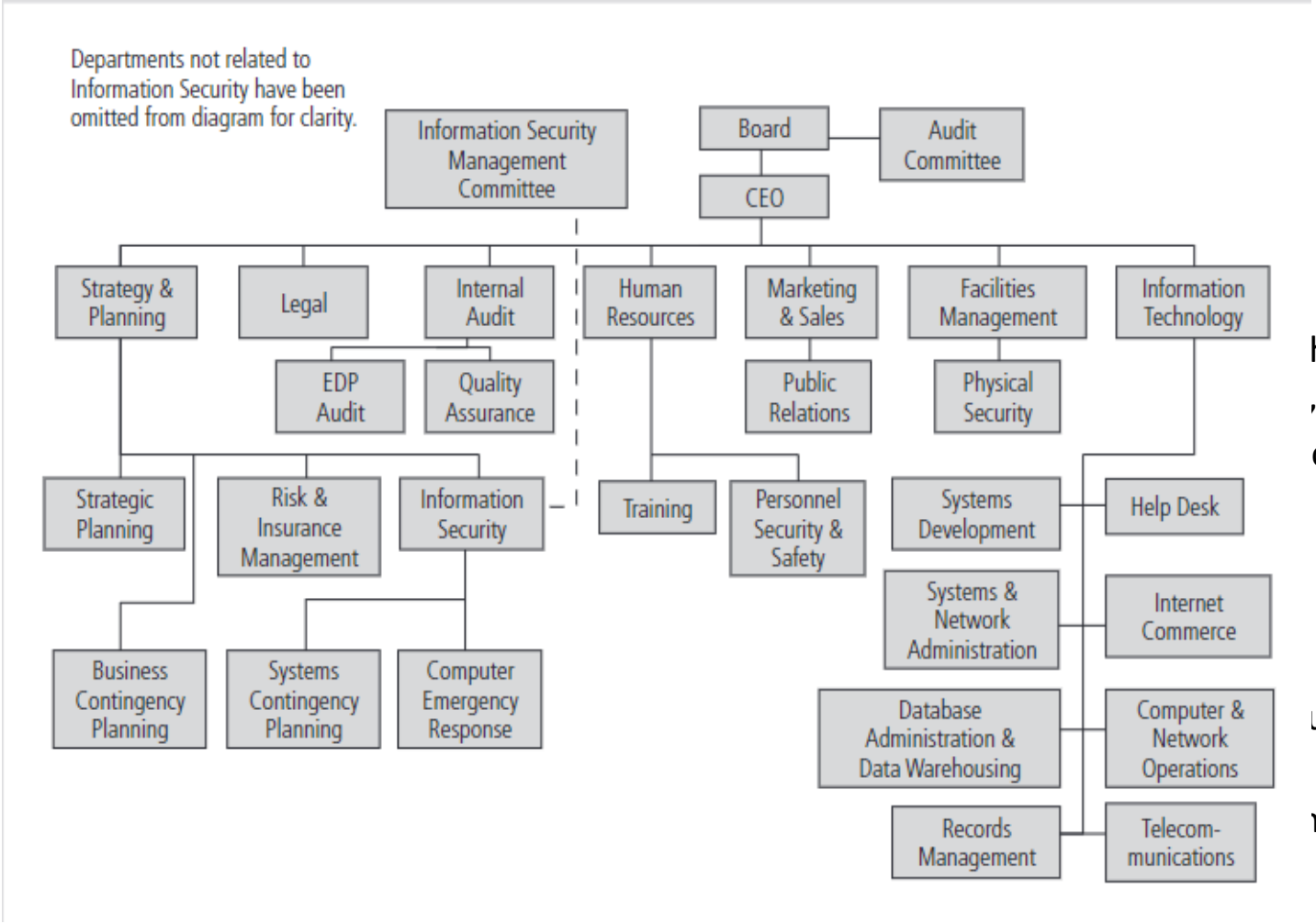
- Quản lý phòng an toàn thông tin báo cáo tới phó chủ tịch

đối với

hông tin
, ...)
on người,

động và
ược

nternet



Các mô hình báo cáo mà các tổ chức thường dùng

Một số lựa chọn khác:

- Trong phòng pháp lý
- Phòng kiểm toán nội bộ báo cáo trực tiếp cho người quản lý IAD
- Thuộc bộ phận trợ giúp
- Trực thuộc phòng kế toán và tài chính, thông qua phòng Công nghệ thông tin đề cập
- Thuộc bộ phận nhân sự
- Báo cáo cho phòng quản lí cơ sở vật chất
- Hướng tiếp cận hoạt động

2. GIỚI THIỆU VỀ CHƯƠNG TRÌNH ĐẢM BẢO ATTT

2.2 Các thành phần của chương trình bảo mật

- Nhu cầu bảo mật thông tin của tổ chức: phù hợp đối với văn hóa, quy mô và ngân sách của công ty.

- Việc xác định mức độ hoạt động của chương trình ATTT phụ thuộc vào kế hoạch chiến lược của tổ chức và cả các tuyên bố về tầm nhìn và sứ mệnh.

2. GIỚI THIỆU VỀ CHƯƠNG TRÌNH ĐẢM BẢO ATTT

2.2 Các thành phần của chương trình bảo mật

- CIO và CISO nên sử dụng hai tài liệu này để xây dựng báo cáo về sứ mệnh cho chương trình an toàn thông tin.

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

  => đưa ra yếu tố thiết yếu và các thành phần của chương trình ATTT mà các tổ chức có thể tham khảo khi tiến hành hoạt động kinh doanh đa tổ chức cũng như kinh doanh nội bộ.

2. GIỚI THIỆU VỀ CHƯƠNG TRÌNH ĐẢM BẢO ATTT

2.2 Các thành phần của chương trình bảo mật

Chính sách	Chính sách chương trình, chính sách cụ thể về vấn đề, chính sách cụ thể của hệ thống
Quản lý chương trình	Chương trình an ninh trung tâm, chương trình cấp hệ thống
Quản lý rủi ro	Đánh giá rủi ro, giảm thiểu rủi ro, phân tích sự không chắc chắn
Lập kế hoạch vòng đời	Kế hoạch bảo mật, giai đoạn bắt đầu, giai đoạn phát triển / mua lại, giai đoạn thực hiện, giai đoạn vận hành / bảo trì
Các vấn đề về nhân sự / người dùng	Nhân sự, quản trị người dùng
Chuẩn bị cho các trường hợp bất thường và thảm họa	Lập kế hoạch kinh doanh, xác định nguồn lực, phát triển kịch bản, phát triển chiến lược, kiểm tra và sửa đổi kế hoạch
Xử lý sự cố bảo mật máy tính	Phát hiện sự cố, phản ứng, phục hồi và theo dõi

2. GIỚI THIỆU VỀ CHƯƠNG TRÌNH ĐẢM BẢO ATTT

2.2 Các thành phần của chương trình bảo mật

Nhận thức và đào tạo	Các kế hoạch SETA, các dự án nâng cao nhận thức và đào tạo về chính sách và thủ tục
Cân nhắc về bảo mật trong hỗ trợ và hoạt động của máy tính	Tích hợp help desk, bảo vệ chống lại kỹ thuật xã hội và cải thiện quản trị hệ thống
An ninh vật lý và môi trường	Bảo vệ, cổng, khóa, và chuông báo động
Nhận dạng và xác thực	Nhận dạng, xác thực, mật khẩu, xác thực nâng cao
Kiểm soát truy cập logic	Tiêu chí truy cập, cơ chế kiểm soát truy cập
Kiểm toán truy vết	Log hệ thống, quy trình xem xét log, hợp nhất và quản lý log
Mật mã học	TKI, VPN, quản lý khóa và khôi phục khóa

2. GIỚI THIỆU VỀ CHƯƠNG TRÌNH ĐẢM BẢO ATTT

2.3 Vai trò và chức danh của ATTT

- **Các vị trí bảo mật thông tin**: chia làm 3 loại:

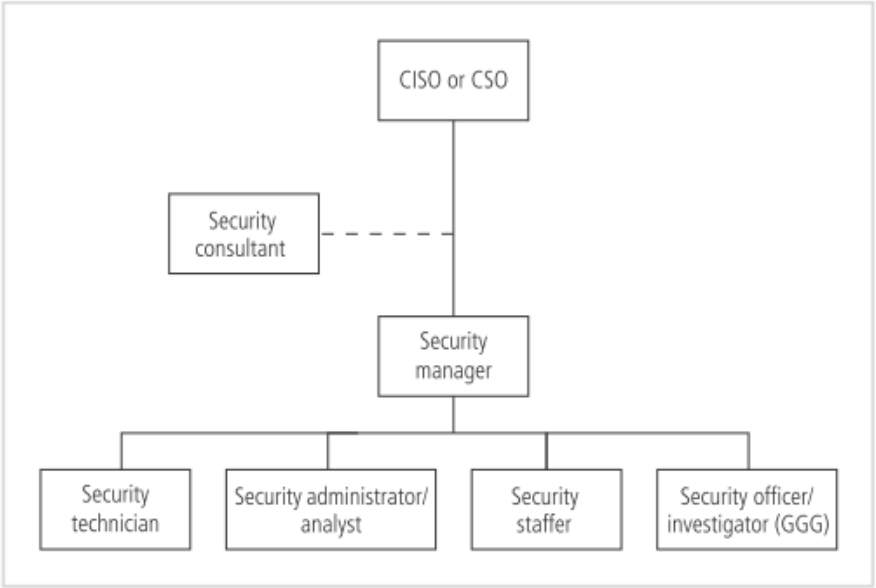
- Để định nghĩa
  - Cung cấp các chính sách, tiêu chuẩn, hướng dẫn, …
  - Tư vấn, đánh giá rủi ro
- Để xây dựng
  - Là các kỹ thuật viên, tạo ra và cài đặt các biện pháp bảo mật
- Để quản trị
  - Giám sát và cải tiến các quy trình bảo mật

2. GIỚI THIỆU VỀ CHƯƠNG TRÌNH ĐẢM BẢO ATTT

2.3 Vai trò và chức danh của ATTT

- **Một tổ chức điển hình** là tổ chức có một số cá nhân có trách nhiệm bảo mật thông tin.

- **Chức danh sử dụng:**
  - Giám đốc An ninh Thông tin (CISO) hoặc Giám đốc An ninh (CSO)
  - Quản lý bảo mật
  - Quản trị viên và phân tích bảo mật
  - Kỹ thuật viên bảo mật
  - Nhân viên bảo mật
  - Cố vấn bảo mật
  - Nhân viên bảo mật, điều tra viên
  - Chuyên viên hỗ trợ



3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ AN NINH (SETA PROGRAM)

- **Chương trình SETA**

  "Là trách nghiệm của CISO và được thiết kế để giảm tỉ lệ vi phạm bảo mật ngẫu nhiên của các thành viên trong tổ chức, bao gồm nhân viên, nhà thầu, nhà tư vấn, nhà cung cấp và đối tác kinh doanh tiếp xúc với tài sản thông tin của tổ chức."

- **SETA đem lại 3 lợi ích chính:**

  - Cải thiện hành vi của nhân viên.
  - Thông báo về các hành vi vi phạm chính sách của các thành viên trong tổ chức.
  - Yêu cầu nhân viên chịu trách nhiệm về các hành vi của mình.

3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ AN NINH (SETA PROGRAM)

- **Mục đích của SETA là tăng cường bảo mật theo 3 cách:**

  - Xây dựng kiến thức chuyên sâu, để thiết kế, triển khai hoặc vận hành các chương trình bảo mật cho các tổ chức và hệ thống.
  - Phát triển các kỹ năng và kiến thức để người dùng máy tính có thể thực hiện công việc của họ trong khi sử dụng hệ thống CNTT an toàn hơn.
  - Nâng cao nhận thức về sự cần thiết phải bảo vệ của tài nguyên hệ thống.

3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ AN NINH (SETA PROGRAM)

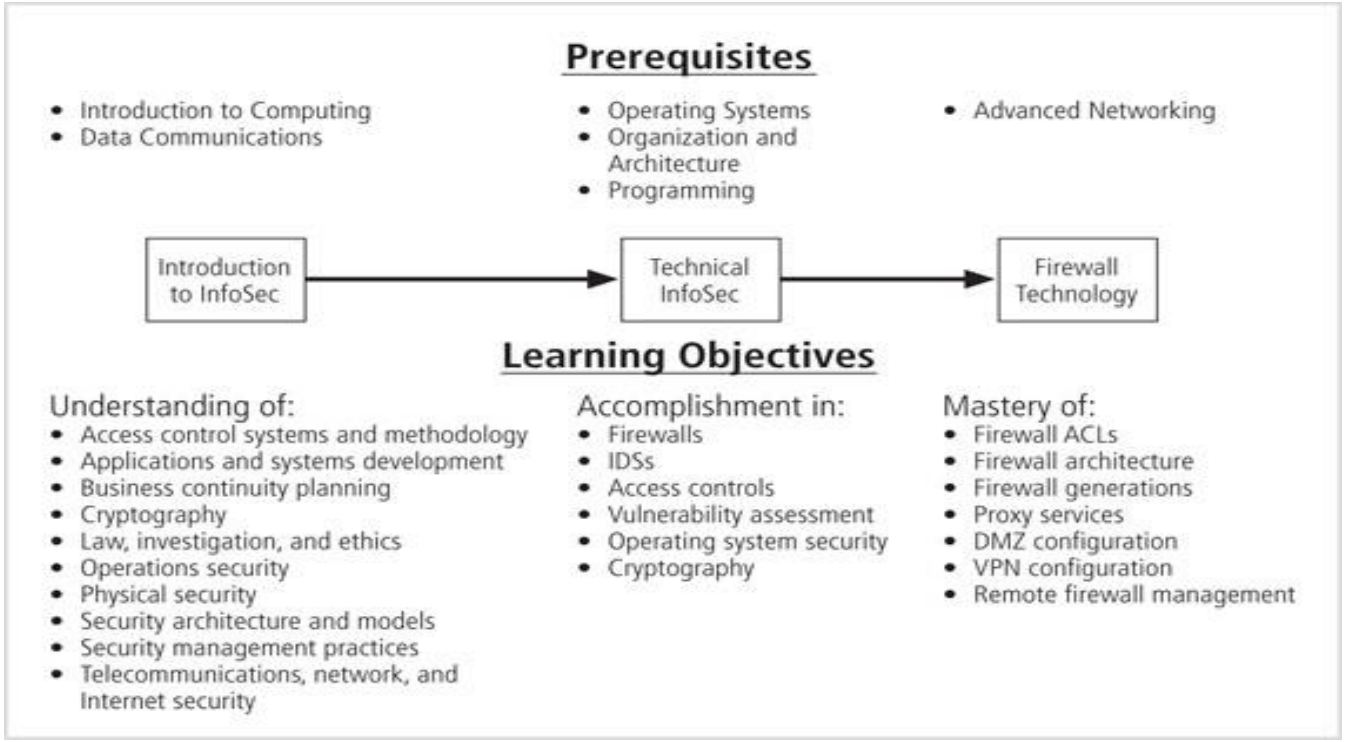
- **Một chương trình SETA bao gồm 3 yếu tố:**
  - Giáo dục bảo mật (**S**ecurity **E**ducation)
  - Đào tạo bảo mật (**T**raning)
  - Nâng cao nhận thức về bảo mật (**A**wareness)

	Awareness	Training	Education
Attribute	"What"	"How"	"Why"
Level	Information	Knowledge	Insight
Objective	Recognition	Skill	Understanding
Teaching Method	• Media Videos • Newsletters • Posters, Inc.	• 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)	Essay (interpret learning)
Impact Timeframe	Short-term	Intermediate	Long-term

3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ BẢO MẬT (SETA PROGRAM)

3.1 SETA: Giáo dục bảo mật

- Nhân viên trong lĩnh vực bảo mật thông tin có thể được khuyến khích học tập chính thức.
- Giáo dục bảo mật là bắt buộc đối với các chuyên gia bảo mật thông tin và là yêu cầu giáo dục phổ thông mà tất cả các chuyên gia IT phải có.
- Một số tổ chức có thể tham khảo các chứng chỉ được cung cấp trong lĩnh vực đó.



3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ AN NINH (SETA PROGRAM)

3.2 Phát triển Giáo dục về bảo mật

- Sau khi các vùng kiến thức được xác định, các vùng kiến thức chung được tổng hợp thành các lĩnh vực dạy học.

- Thiết kế khóa học:

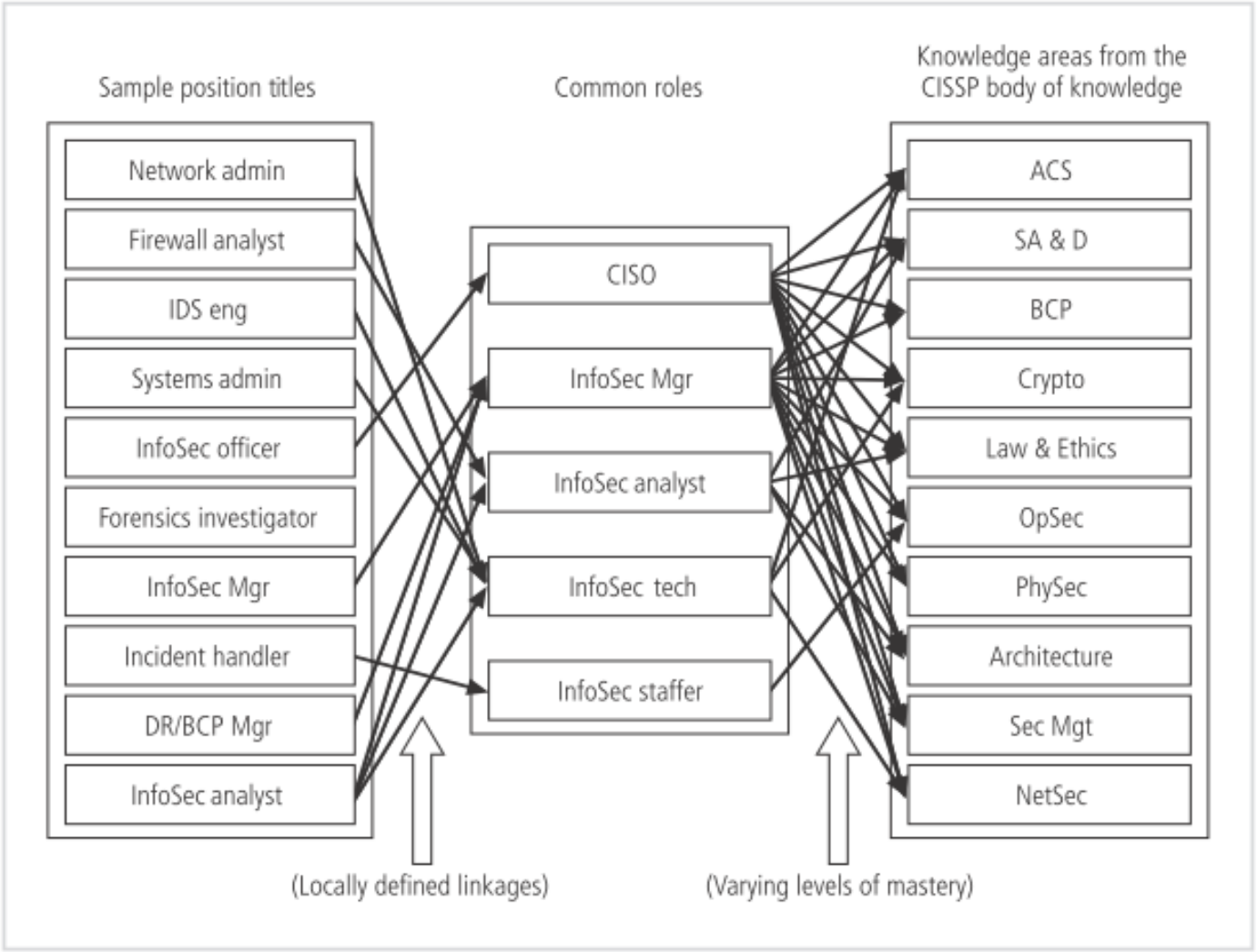
  - Nên cho phép học sinh đạt được kiến thức và kỹ năng cần thiết sau khi hoàn thành chương trình.

  - Xác định kiến thức tiên quyết cho mỗi lớp.

3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ AN NINH (SETA PROGRAM)

3.2 Phát triển Giáo dục về bảo mật

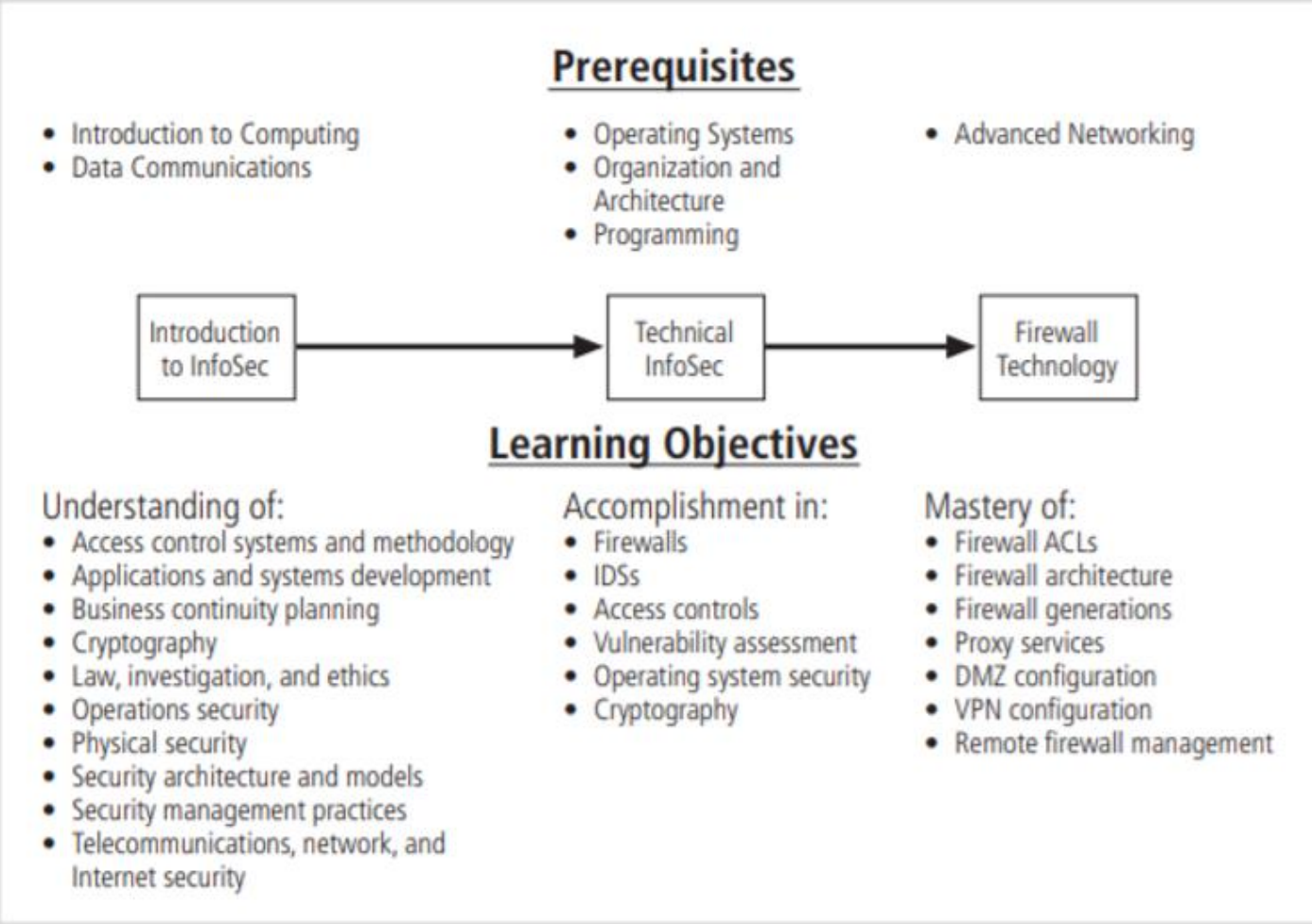
- Bản đồ kiến thức trong an toàn thông tin



3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ AN NINH (SETA PROGRAM)

3.2 Phát triển Giáo dục về bảo mật

- Biểu đồ mô tả các tiến trình của 1 khóa cùng cùng với các lĩnh vực kiến thức và yêu cầu tiên quyết.



3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ AN NINH (SETA PROGRAM)

3.3 SETA: Đào tạo an ninh

- Liên quan đến việc cung cấp thông tin chi tiết và hướng dẫn thực hành.

- Ban quản lý có thể phát triển đào tạo tùy chỉnh hoặc thuê ngoài

- Có 2 phương pháp đào tạo cho người dùng
  - Theo nền tảng chức năng: người dùng thông thường, quản lý, người dùng kỹ thuật
  - Theo trình độ kỹ năng: người mới, trung cấp, nâng cao

3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ AN NINH (SETA PROGRAM)

3.4 SETA: Kỹ thuật đào tạo

- Sử dụng sai phương pháp có thể cản trở việc chuyển giao kiến thức.
- Cần chương trình đào tạo tốt.
- Việc đào tạo dành cho một hoặc một vài cá nhân.
- Lựa chọn phương pháp đào tạo (Không phải lúc nào cũng dựa trên kết quả tốt nhất của học viên)

Các loại phương thức đào tạo	
One –on –One	Computer – based training (CBT)
Formal Class	Distance learning & web seminars
On – the –job training	Seft – study (non - computerized)
User support group	Serious Games

3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ AN NINH (SETA PROGRAM)

3.4 SETA: Kỹ thuật đào tạo

- Việc triển khai đào tạo thông thường được áp dụng thông qua 7 bước:

  - ✓ Bước 1: Xác định phạm vi, mục tiêu và mục tiêu của chương trình.
  - ✓ Bước 2: Xác định nhân viên đào tạo.
  - ✓ Bước 3: Xác định đối tượng mục tiêu.
  - ✓ Bước 4: Tạo động lực cho quản lý và nhân viên.
  - ✓ Bước 5: Quản trị chương trình.
  - ✓ Bước 6: Duy trì chương trình.
  - ✓ Bước 7: Đánh giá chương trình.

3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ AN NINH (SETA PROGRAM)

3.5 SETA: Nhận thức về bảo mật

"Một trong những phương pháp bảo mật ít được thực hiện nhất nhưng hiệu quả nhất là chương trình nâng cao nhận thức về bảo mật"

- Tạo tiền đề cho việc đào tạo bằng cách thay đổi thái độ của tổ chức để nhận ra tầm quan trọng của an ninh và những hậu quả bất lợi khi các chương trình an ninh không đạt hiệu quả
- Nhắc nhở người dùng về các quy trình cần tuân thủ

3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ AN NINH (SETA PROGRAM)

3.5 SETA: Nhận thức về bảo mật

- Các cách thức thực hành tốt nhất:
  - Tập trung vào con người.
  - Không sử dụng thuật ngữ kỹ thuật.
  - Sử dụng mọi địa điểm có sẵn.
  - Xác định mục tiêu học tập, trình bày rõ ràng, cung cấp đầy đủ chi tiết và phạm vi
  - Giữ mọi thứ nhẹ nhàng.
  - Đừng làm quá tải người dùng.
  - Giúp người dùng hiểu vai trò của họ trong InfoSec.
  - Tận dụng các phương tiện truyền thông nội bộ.
  - Tạo những chương trình nhận thức chính thức. Lập kế hoạch và ghi lại tất cả các hoạt động.
  - Cung cấp thông tin tốt sớm chứ không phải là thông tin hoàn hảo nhưng muộn.

3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ AN NINH (SETA PROGRAM)

3.5 SETA: Nhận thức về bảo mật

- Lời khuyên cho các chương trình đào tạo nhận thức về ATTT
  - Bảo mật thông tin là vấn đề của mọi người.
  - Sử dụng ngôn ngữ dễ hiểu. Nếu họ không thể hiểu nó, họ sẽ khó học nó.
  - Đưa ra quan điểm bản thân, ủng hộ nó và kết luận nó.
  - Luôn cho người dùng nhận biết hành vi mà bạn yêu cầu sẽ ảnh hưởng tới họ như thế nào.
  - Chính thức hoá phương pháp đào tạo của bản thân.
  - Luôn có mặt kịp thời.

3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ AN NINH (SETA PROGRAM)

3.5 SETA: Nhận thức về bảo mật

- Chương trình cần được thiết kế để sửa đổi bất kỳ hành vi nào của nhân viên gây nguy hiểm cho bảo mật thông tin của tổ chức.
- Các chương trình hiệu quả khiến nhân viên có trách nhiệm với hành động của họ.
- Nhận thức về bảo mật cần được phổ biến và thực thi giúp các chính sách trở nên dễ dàng hơn.
- Chứng minh sự quan tâm và thẩm định đúng mức có thể giúp tổ chức tránh khỏi các vụ kiện.

3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ AN NINH (SETA PROGRAM)

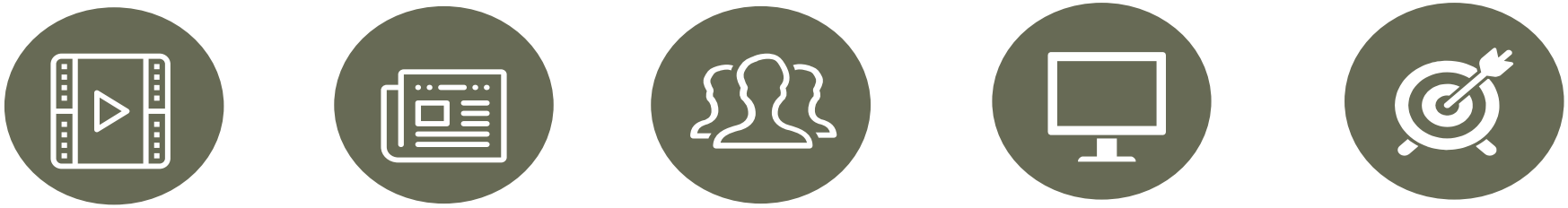
3.5 SETA: Nhận thức về bảo mật

- Nhận thức có thể có nhiều dạng khác nhau đối với các đối tượng cụ thể.
- Một chương trình nâng cao nhận thức về bảo mật có thể sử dụng nhiều phương pháp để truyền tải thông điệp của nó.
- Chỉ ra rằng mọi người có xu hướng thực hành một quá trình điều chỉnh (thích nghi).

3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ AN NINH (SETA PROGRAM)

3.5 SETA: Nhận thức về bảo mật

"Nhiều thành phần nâng cao nhận thức về bảo mật có sẵn với chi phí thấp hoặc miễn phí"



Video	Áp phích và biểu ngữ	Bài giảng, hội nghị	Đào tạo dựa trên máy	Trò chơi

3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ AN NINH (SETA PROGRAM)

3.5 SETA: Nhận thức về bảo mật

Poster, bảng tin về bảo mật

Phụ kiện

3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ AN NINH (SETA PROGRAM)

3.5 SETA: Nhận thức về bảo mật

Quà lưu niệm

3. TRIỂN KHAI CÁC CHƯƠNG TRÌNH GIÁO DỤC, ĐÀO TẠO VÀ NHẬN THỨC VỀ AN NINH (SETA PROGRAM)

3.5 SETA: Nhận thức về bảo mật

- Trang web nhận thức về bảo mật thông tin

- Một trang Web giáo dục tốt
  - Tìm kiếm những gì đã có sẵn
  - Lập kế hoạch
  - Thời gian tải trang phải là tối thiểu
  - Tìm kiếm phản hồi
  - Giả sử không có gì và kiểm tra mọi thứ
  - Dành thời gian quảng bá trang Web

Tóm tắt

- Tổ chức bảo mật
- Đặt bảo mật thông tin trong một tổ chức
- Các thành phần của chương trình bảo mật
- Vai trò và chức danh bảo mật thông tin
- Thực hiện các chương trình giáo dục, đào tạo và nâng cao nhận thức về an ninh