ĐẢM BẢO VÀ AN TOÀN THÔNG TIN (INFORMATION ASSURANCE AND SECURITY)

BÀI 1: GIỚI THIỆU VỀ AN TOÀN THÔNG TIN

GIÁO VIÊN: ĐẶNG LÊ ĐÌNH TRANG

BỘ MÔN ATTT – KHOA CNTT

NHÀ S1, PHÒNG 2203

GIỚI THIỆU MÔN HỌC

- Tên học phần: Đảm bảo an toàn thông tin.
- Số tín chỉ: 3TC, Số tiết (lý thuyết, thực hành) – (30, 15)
- Học phần bắt buộc
- Nội dung:
  - Định nghĩa về an toàn thông tin, những khái niệm cơ
  - Các nguy cơ đối với hệ thống thông tin
  - Giới thiệu một số giải phải đảm bảo an toàn thông tin cho hệ thống (tường lửa, mạng lan ảo (VPN), hệ thống phát hiện xâm nhập (IDS), hệ thống ngăn chặn xâm nhập (IPS).
  - Giới thiệu một số mô hình mã hóa cổ điển, cơ bản về chữ ký số. Bảo mật về mặt vật lý.

TÀI LIỆU THAM KHẢO

- Principles of Information Security - Michael E. Whitman and Herbert J. Matord
- Information Security Fundamentals - Thomas R. Peltier, Justin Peltier
- Cryptography: Theory and Practice - Douglas Stinson
- Introduction to Computer Security, Matt Bishop
- Google, Wikipedia, ...

BÀI 1: GIỚI THIỆU VỀ AN TOÀN THÔNG TIN

"A WELL-INFORMED SENSE OF ASSURANCE THAT THE INFORMATION RISKS AND CONTROLS ARE IN BALANCE." —JAMES M. ANDERSON, EMAGINED

NỘI DUNG

1. Lịch sử bảo mật thông tin
2. Khái niệm về bảo mật thông tin
3. Mô hình bảo mật CNSS
4. Các thành phần của một hệ thống thông tin
5. Cân bằng giữa bảo mật và khả năng truy cập
6. Các phương án triển khai bảo mật thông tin
7. Bảo mật trong vòng đời của hệ thống
8. Câu hỏi ôn tập

NỘI DUNG

1. **Lịch sử bảo mật thông tin**
2. Khái niệm về bảo mật thông tin
3. Mô hình bảo mật CNSS
4. Các thành phần của một hệ thống thông tin
5. Cân bằng giữa bảo mật và khả năng truy cập
6. Các phương án triển khai bảo mật thông tin
7. Bảo mật trong vòng đời của hệ thống
8. Câu hỏi ôn tập

1. LỊCH SỬ BẢO MẬT THÔNG TIN

- Tại sao cần đảm bảo bảo mật thông tin?
- Thông tin có phải một loại tài sản?
- Giá trị của thông tin?
- Hình thức của thông tin?

1. LỊCH SỬ BẢO MẬT THÔNG TIN

- Vì thông tin là một loại tài sản, nó liên quan tới các tài sản vật lý (tiền, vàng, bất động sản, …)
- Thông tin là một loại tài sản (thông tin khách hàng, cơ sở dữ liệu, …
- Phụ thuộc vào mức độ liên quan tới các loại tài sản vật lý
- Text, media, …

1. LỊCH SỬ BẢO MẬT THÔNG TIN

- Thuở sơ khai của bảo mật thông tin: đảm bảo an toàn vật lý
- Các nguy cơ vật lý là gì?

1. LỊCH SỬ BẢO MẬT THÔNG TIN

- Thuở sơ khai của bảo mật thông tin: đảm bảo an toàn vật lý
- Trộm cắp tài sản
- Thiên tai bão lũ, chiến tranh, …

1. LỊCH SỬ BẢO MẬT THÔNG TIN

- Cùng với sự phát triển của máy tính, mạng internet, …
  - Thông tin lưu trữ trên các thiết bị điện tử
  - Truy cập từ xa
- Các nguy cơ về an toàn bảo mật thông tin phi vật lý?

1. LỊCH SỬ BẢO MẬT THÔNG TIN

- Cùng với sự phát triển của máy tính, mạng internet, …
  - Thông tin lưu trữ trên các thiết bị điện tử
  - Truy cập từ xa
- Các nguy cơ về an toàn bảo mật thông tin phi vật lý:
  - Gửi nhầm file
  - Nghe trộm
  - Truy cập trái phép, …

NỘI DUNG

1. Lịch sử bảo mật thông tin
2. Khái niệm về bảo mật thông tin
3. Mô hình bảo mật CNSS
4. Các thành phần của một hệ thống thông tin
5. Cân bằng giữa bảo mật và khả năng truy cập
6. Các phương án triển khai bảo mật thông tin
7. Bảo mật trong vòng đời của hệ thống
8. Câu hỏi ôn tập

2. KHÁI NIỆM VỀ BẢO MẬT THÔNG TIN

- Bảo mật là gì?

2. KHÁI NIỆM VỀ BẢO MẬT THÔNG TIN

- Chất lượng hay trạng thái an toàn – Không bị nguy hiểm
- Có nhiều lớp bảo mật
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security
  - Information security

2. KHÁI NIỆM VỀ BẢO MẬT THÔNG TIN

- Là sự bảo vệ thông tin cũng như các thành phần của nó, bao gồm hệ thống, phần cứng được dùng để sử dụng, lưu trữ, chuyển tải thông tin đó
- Information security (infosec) is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information
- Information security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information

NỘI DUNG

1. Lịch sử bảo mật thông tin
2. Khái niệm về bảo mật thông tin
3. Mô hình bảo mật CNSS
4. Các thành phần của một hệ thống thông tin
5. Cân bằng giữa bảo mật và khả năng truy cập
6. Các phương án triển khai bảo mật thông tin
7. Bảo mật trong vòng đời của hệ thống
8. Câu hỏi ôn tập

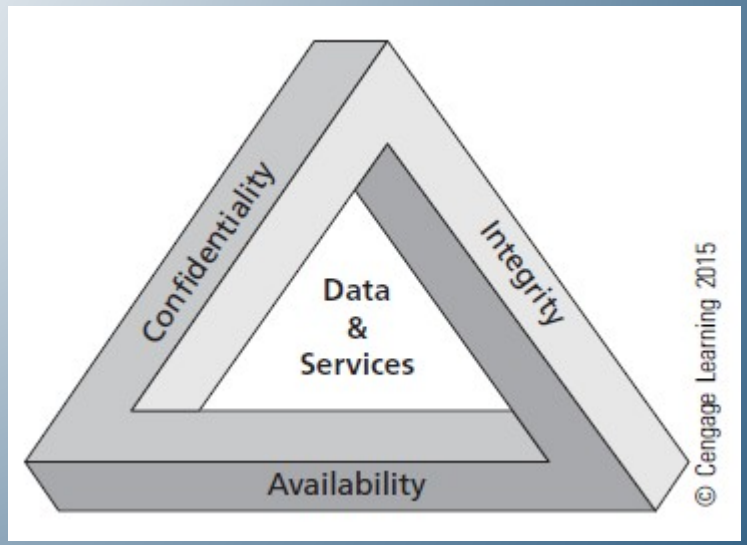
3. MÔ HÌNH BẢO MẬT CNSS

- Thông tin có những đặc tính gì?

3. MÔ HÌNH BẢO MẬT CNSS

- Chúng ta bắt đầu bằng một khái niệm về bảo mật máy tính, đó là mô hình tam giác C.I.A.
- Dựa trên ba đặc tính của thông tin:
  - C: Tính bảo mật
  - I: Tính toàn vẹn
  - A: Tính sẵn sàng
- Tuy nhiên mô hình này không còn thích hợp khi áp dụng trong môi trường mới
  - Các mối de dọa phức tạp và đa dạng hơn
  - Các nguy cơ ngẫu nhiên: thiên tai, trộm cắp

Ⓟ Cần một mô hình mở rộng hơn



3. MÔ HÌNH BẢO MẬT CNSS

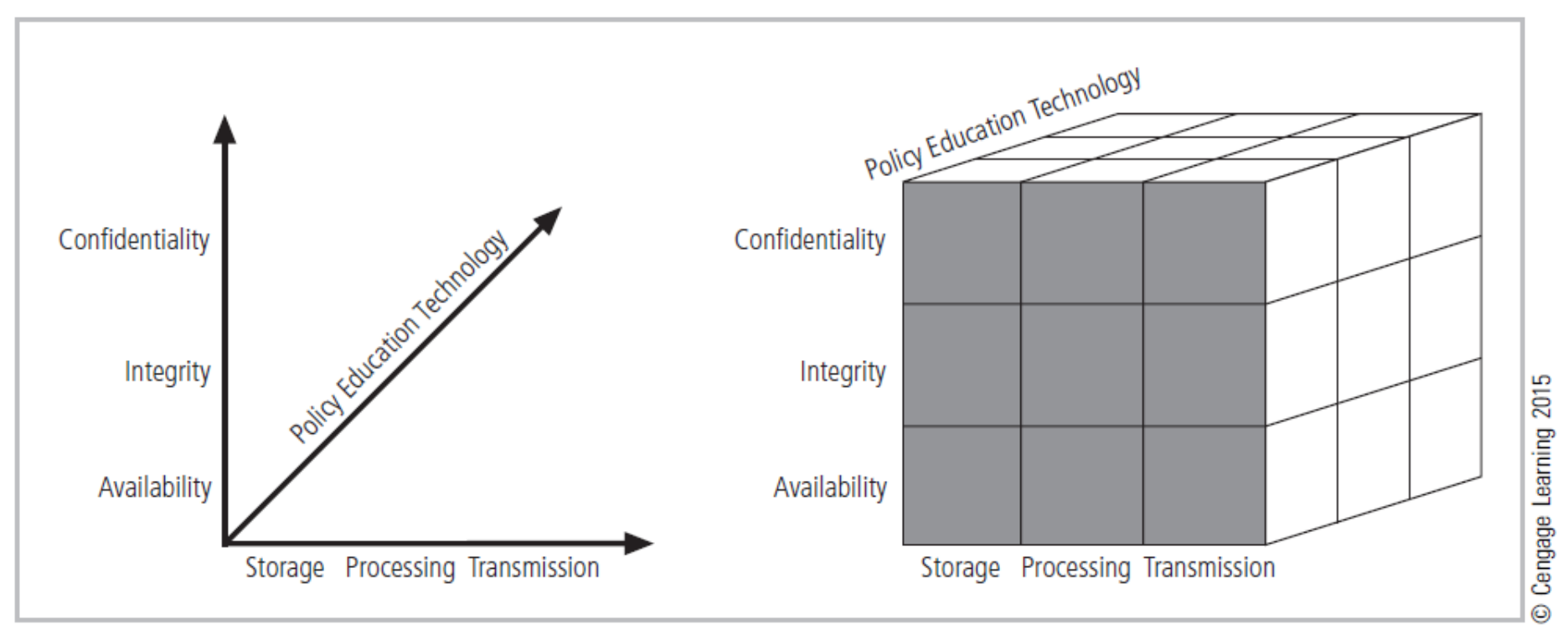
- Giá trị của thông tin đến từ các đặc tính của nó.
  - Tính kịp thời
  - Sẵn sàng
  - Độ chính xác
  - Tính xác thực
  - Tính bảo mật
  - Đồng nhất
  - Khả dụng
  - Sở hữu

3. MÔ HÌNH BẢO MẬT CNSS

- Giá trị của thông tin đến từ các đặc tính của nó.
  - Tính kịp thời: Sẽ không có giá trị nếu thông tin đến quá muộn
  - Sẵn sàng: Người dùng khó tiếp cận với thông tin khi cần
  - Độ chính xác: Không được phép có lỗi
  - Tính xác thực: Rõ nguồn gốc
  - Tính bảo mật: Không lộ, lọt tới những đối tượng không được phép
  - Tính đồng nhất:
  - Khả dụng
  - Sở hữu

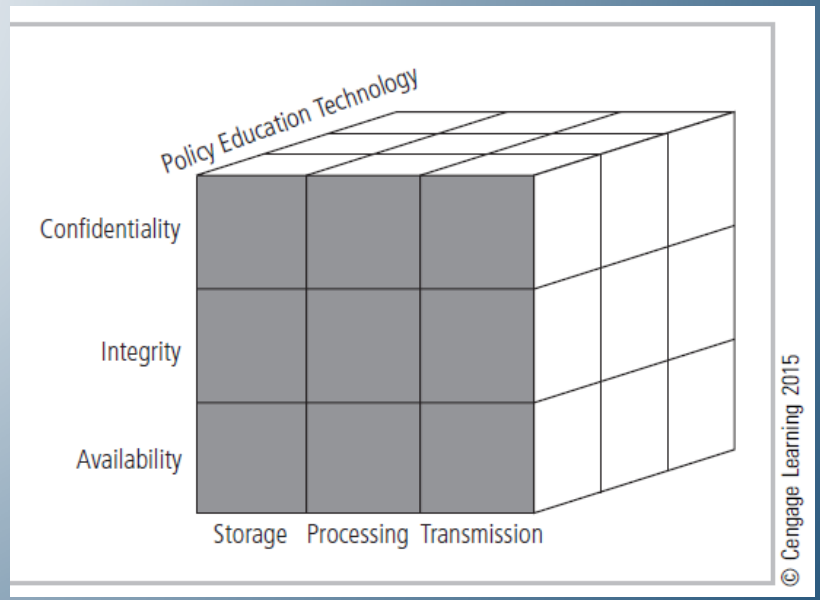
3. MÔ HÌNH BẢO MẬT CNSS

- Committee on National Security Systems (CNSS)



3. MÔ HÌNH BẢO MẬT CNSS

- Mô hình 3 chiều, gồm 27 khối
- Mỗi khối đại diện cho một mảng trong bảo mật thông tin hiện đại
- Ví dụ: giao của technology, integrity, và storage là mảng bảo vệ ứng dụng công nghệ để đảm bảo tính toàn vẹn của thông tin trong lưu trữ
- Các bạn sinh viên diễn đạt vài ví dụ khác



NỘI DUNG

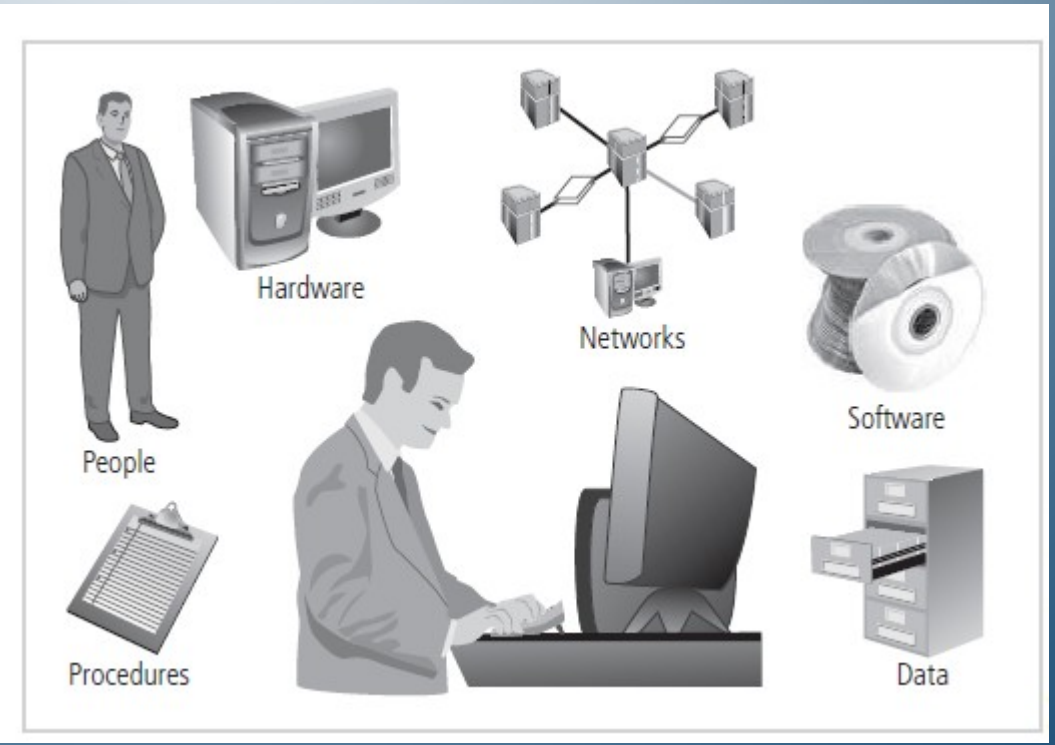
1. Lịch sử bảo mật thông tin
2. Khái niệm về bảo mật thông tin
3. Mô hình bảo mật CNSS
4. Các thành phần của một hệ thống thông tin
5. Cân bằng giữa bảo mật và khả năng truy cập
6. Các phương án triển khai bảo mật thông tin
7. Bảo mật trong vòng đời của hệ thống
8. Câu hỏi ôn tập

4. CÁC THÀNH PHẦN CỦA MỘT HỆ THỐNG THÔNG TIN

- Một hệ thống thông tin gồm những thành phần nào?

4. CÁC THÀNH PHẦN CỦA MỘT HỆ THỐNG THÔNG TIN

- Một hệ thống thông tin gồm những thành phần nào?
  - Con người
  - Thiết bị phần cứng
  - Mạng
  - Phần mềm
  - Dữ liệu
  - Các thủ tục



4. CÁC THÀNH PHẦN CỦA MỘT HỆ THỐNG THÔNG TIN

- Các thành phần của bảo mật thông tin

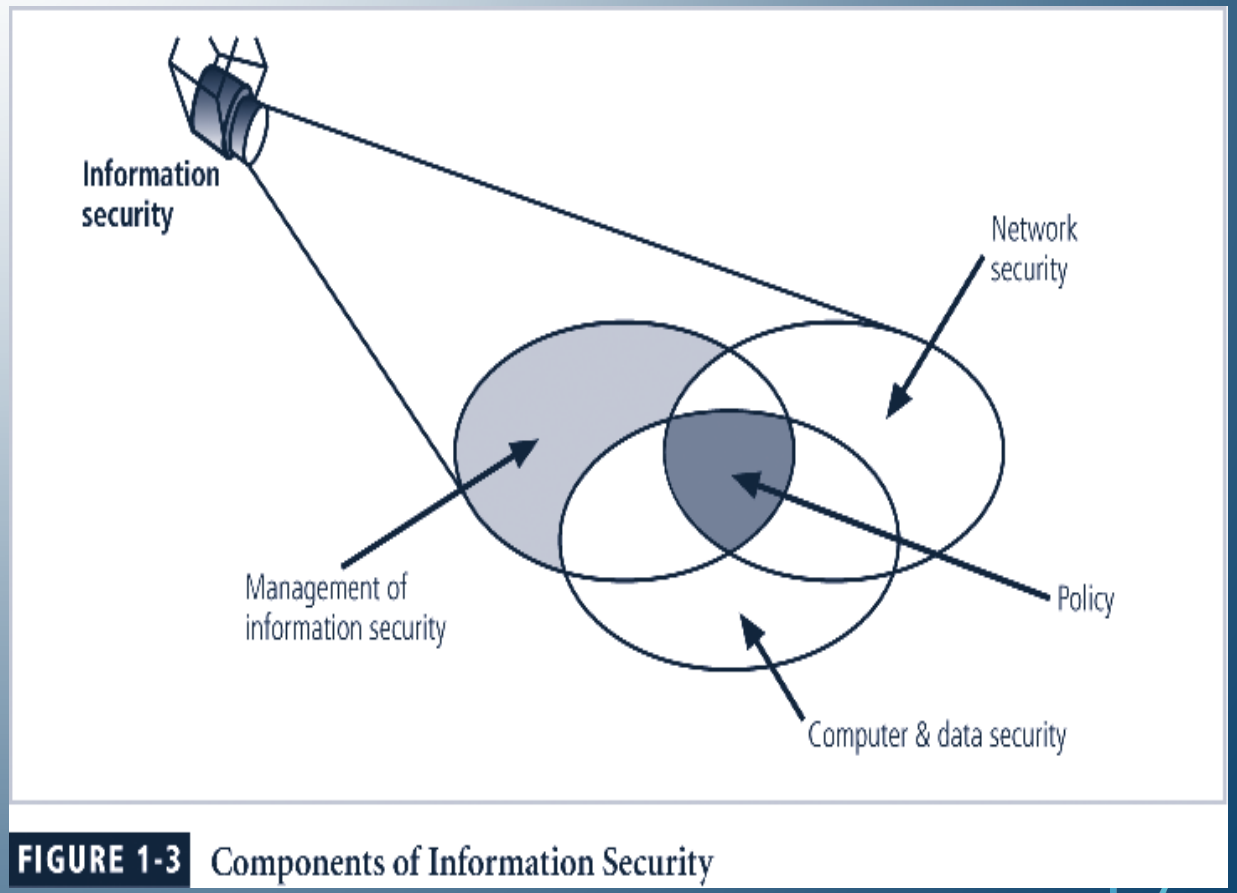


FIGURE 1-3 Components of Information Security

NỘI DUNG

1. Lịch sử bảo mật thông tin
2. Khái niệm về bảo mật thông tin
3. Mô hình bảo mật CNSS
4. Các thành phần của một hệ thống thông tin
5. Cân bằng giữa bảo mật và khả năng truy cập
6. Các phương án triển khai bảo mật thông tin
7. Bảo mật trong vòng đời của hệ thống
8. Câu hỏi ôn tập

5. CÂN BẰNG GIỮA BẢO MẬT VÀ KHẢ NĂNG TRUY CẬP

- Một hệ thống bảo mật hoàn hảo có tồn tại?
- “A well-informed sense of assurance that the information risks and controls are in balance.” —James M. Anderson, emagined
- Ví dụ: Hệ thống email nội bộ trong HV, quy định rằng tất cả các văn bản gửi đi đều phải được mã hóa
  - Ⓟ Vấn đề gì với hệ thống này?

5. CÂN BẰNG GIỮA BẢO MẬT VÀ KHẢ NĂNG TRUY CẬP

- Ví dụ: Hệ thống email nội bộ trong HV, quy định rằng tất cả các văn bản gửi đi đều phải được mã hóa
  - Bảo mật cao, an toàn
  - Phiền toái với người dùng
  - Áp lực lên các hệ thống phần cứng

➔Bái toàn về sự cân bằng giữ yếu tố bảo mật và khả năng truy cập của một hệ thống mà lời giải phụ thuộc rất nhiều yếu tố:

- Tính chất của tổ chức
- Cơ sở hạ tầng kỹ thuật
- Thời gian, …

Ⓟ Việc triển khai các hệ thống bảo mật thông tin là luôn thay đổi!

NỘI DUNG

1. Lịch sử bảo mật thông tin
2. Khái niệm về bảo mật thông tin
3. Mô hình bảo mật CNSS
4. Các thành phần của một hệ thống thông tin
5. Cân bằng giữa bảo mật và khả năng truy cập
6. Các phương án triển khai bảo mật thông tin
7. Bảo mật trong vòng đời của hệ thống
8. Câu hỏi ôn tập

6. CÁC PHƯƠNG ÁN TRIỂN KHAI BẢO MẬT THÔNG TIN

- Yêu cầu cho các hệ thống thông tin luôn luôn thay đổi. Vì sao?
- Việc triển khai bảo mật thông tin là thường xuyên liên tục. Phương thức triển khai như thế nào?

6. CÁC PHƯƠNG ÁN TRIỂN KHAI BẢO MẬT THÔNG TIN

- Yêu cầu cho các hệ thống thông tin luôn luôn thay đổi. vì:
  - Các yếu tố nguy cơ luôn luôn phát sinh, biến đổi
  - Sự cân bằng (mục 5)
- Việc triển khai bảo mật thông tin là thường xuyên liên tục. Phương thức triển khai:
  - Tiếp cận từ trên xuống dưới
  - Tiếp cận từ dưới lên trên

6. CÁC PHƯƠNG ÁN TRIỂN KHAI BẢO MẬT THÔNG TIN

- Trên xuống dưới:
  - Bắt đầu từ các vấn đề trong chính sách, thủ tục và quy trình
  - Đặt ra các mục tiêu đầu ra cho dự án
  - Xác định cụ thể các hành động

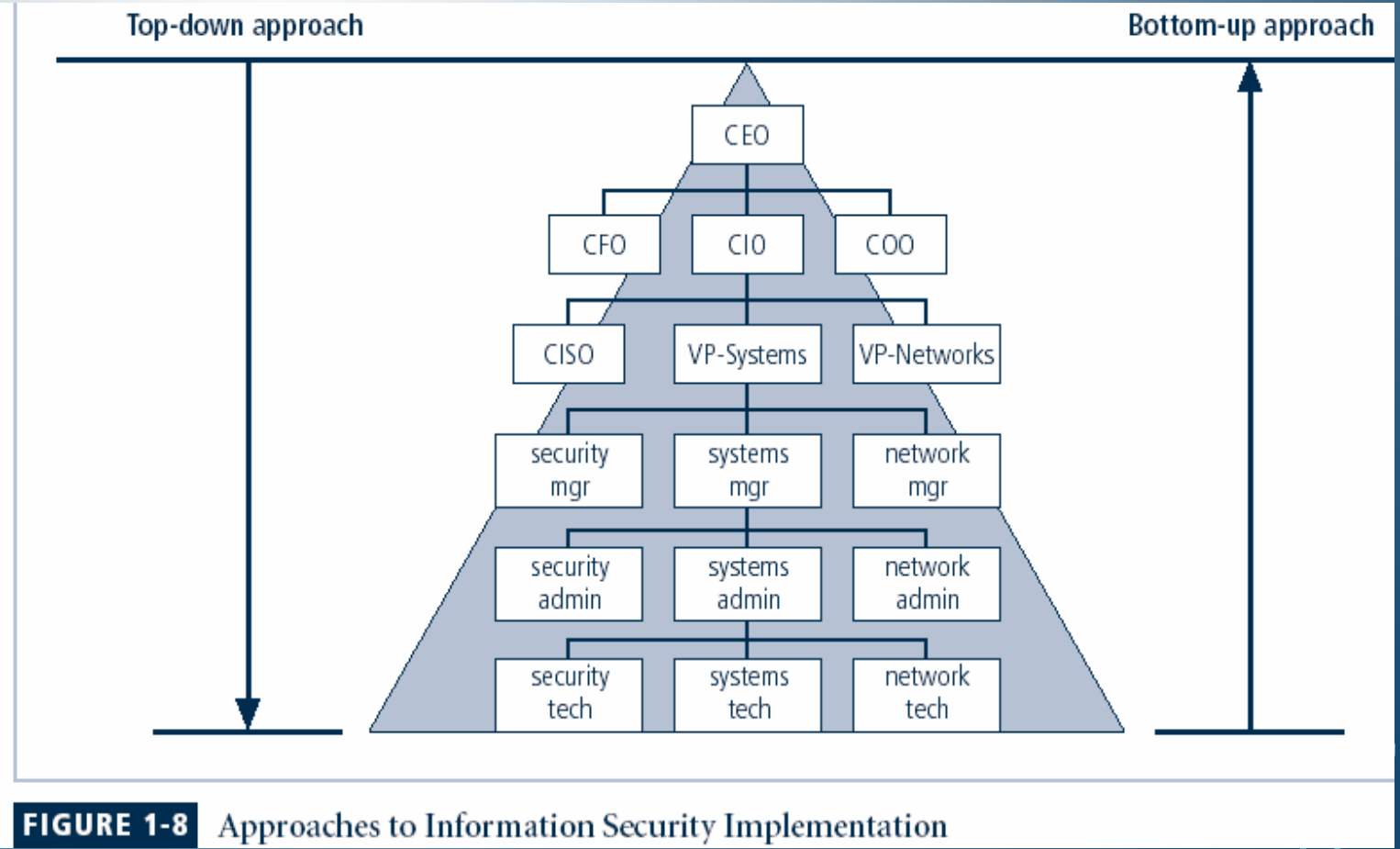


FIGURE 1-8 Approaches to Information Security Implementation

6. CÁC PHƯƠNG ÁN TRIỂN KHAI BẢO MẬT THÔNG TIN

- Dưới lên trên: nhà quản trị hệ thống tiến hành các cải tiến nhằm năng cao chất lượng của hệ thống

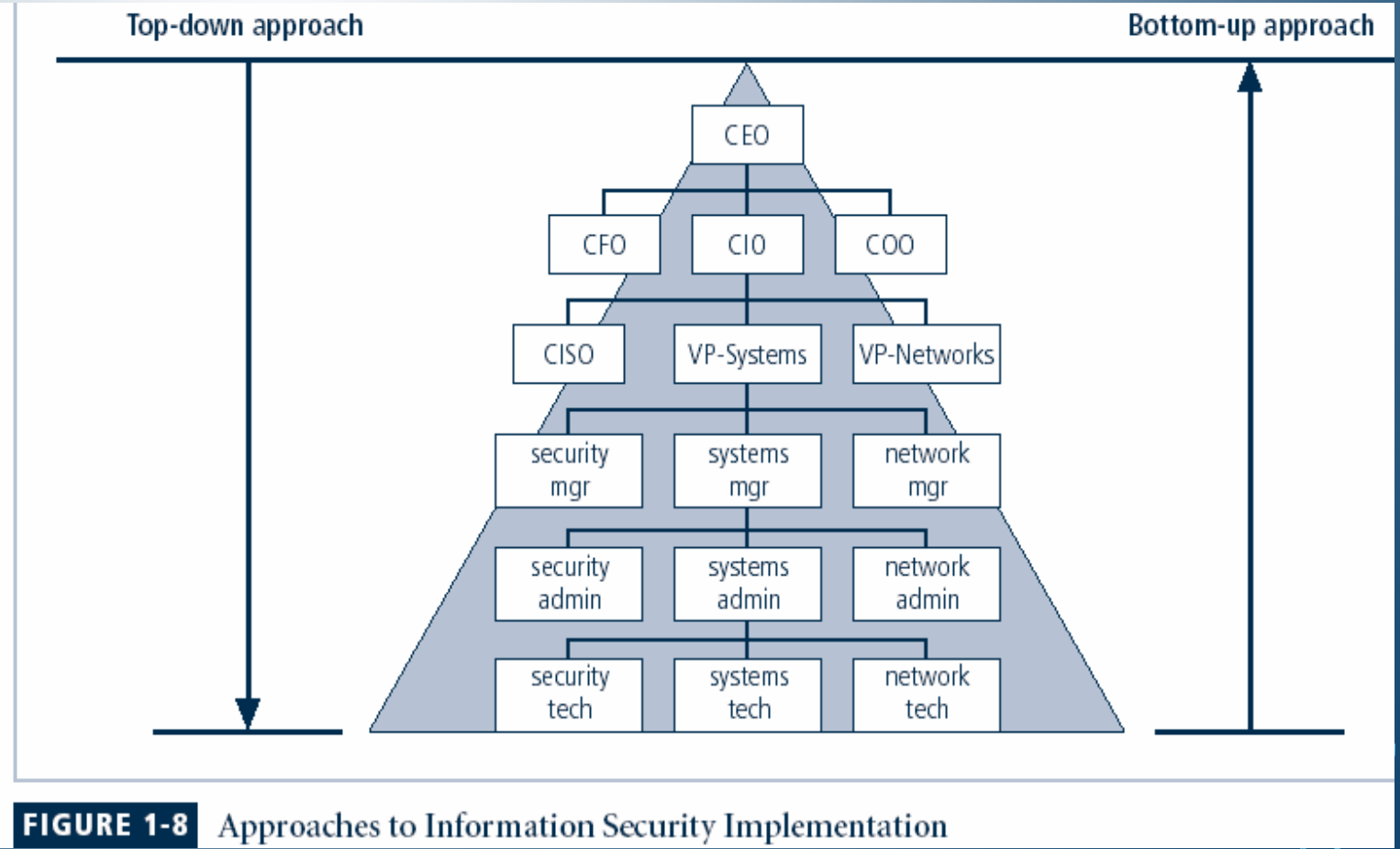


FIGURE 1-8 Approaches to Information Security Implementation

NỘI DUNG

1. Lịch sử bảo mật thông tin
2. Khái niệm về bảo mật thông tin
3. Mô hình bảo mật CNSS
4. Các thành phần của một hệ thống thông tin
5. Cân bằng giữa bảo mật và khả năng truy cập
6. Các phương án triển khai bảo mật thông tin
7. Bảo mật trong vòng đời của hệ thống
8. Câu hỏi ôn tập

7. BẢO MẬT TRONG VÒNG ĐỜI CỦA HỆ THỐNG

- systems development life cycle (SDLC)
- Phương pháp SDLC waterfall

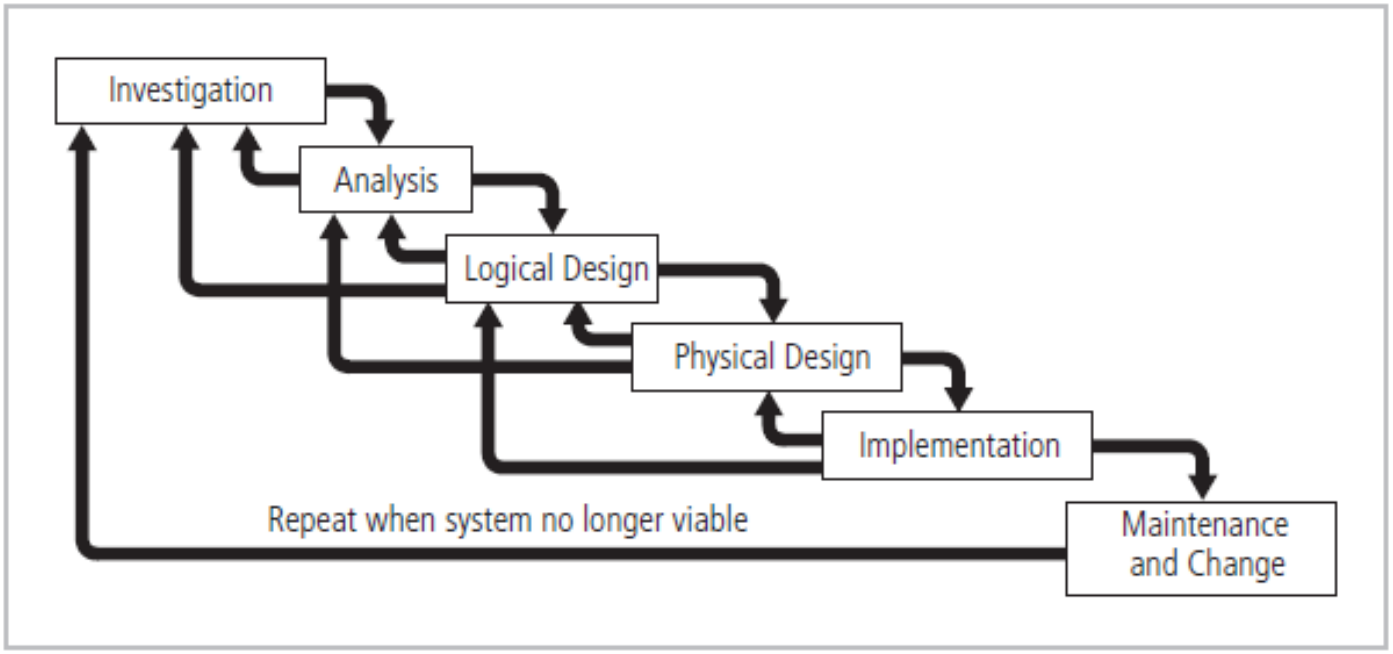


Figure 1-13 SDLC waterfall methodology

7. BẢO MẬT TRONG VÒNG ĐỜI CỦA HỆ THỐNG

- Đặt vấn đề
- Phân tích
- Thiết kế logic
- Thiết kế vật lý
- Triển khai
- Bảo trì và sửa đổi

Ⓟ Yếu tố bảo mật áp dụng thế nào trong SDLC

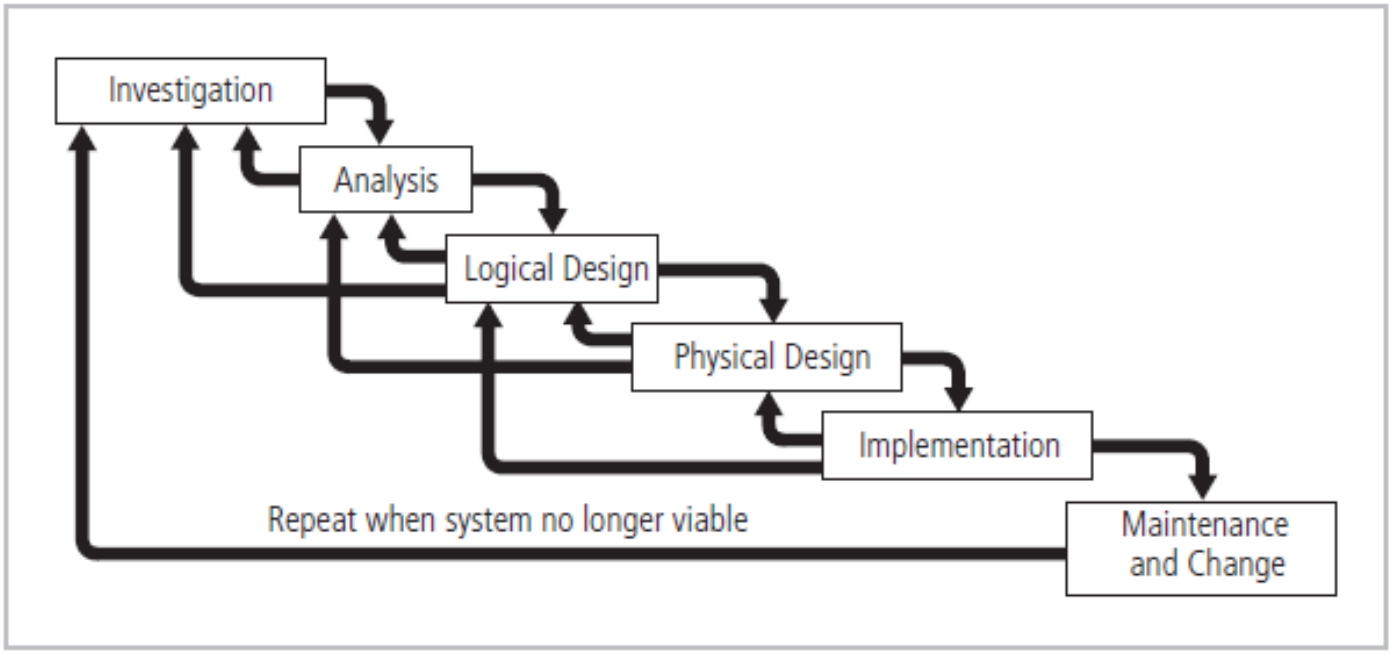


Figure 1-13 SDLC waterfall methodology

7. BẢO MẬT TRONG VÒNG ĐỜI CỦA HỆ THỐNG

- Phương pháp SecSDLC
  - Đặt vấn đề: bổ sung các chính sách bảo mật, cân đối tài chính dành cho bảo mật
  - Phân tích: Hiểu rõ các vấn đề liên quan tới bảo mật, phần tích xác định các rủi ro cho hệ thống
  - Thiết kế logic: Phát triển các bản vẽ bảo mật, dự trù các hành động ứng phó
  - Thiết kế vật lý: lựa chọn công nghệ, giải pháp
  - Triển khai
  - Bảo trì và sửa đổi

NỘI DUNG

1. Lịch sử bảo mật thông tin
2. Khái niệm về bảo mật thông tin
3. Mô hình bảo mật CNSS
4. Các thành phần của một hệ thống thông tin
5. Cân bằng giữa bảo mật và khả năng truy cập
6. Các phương án triển khai bảo mật thông tin
7. Bảo mật trong vòng đời của hệ thống
8. Câu hỏi ôn tập

8. CÂU HỎI ÔN TẬP: TÌM HIỂU CÁC TỪ KHÓA

- Access
- Asset
- Attack
- Control, Safeguard or Countermeasure
- Exploit
- Exposure
- Hacking
- Object
- Risk
- Security Blueprint
- Security Model
- Security Posture or Security Profile
- Subject
- Threats
- Threat Agent
- Vulnerability

REFERENCE

- Why we need a new definition of information security - James M. Anderson, CISSP