BÀI 1

TỔNG QUAN VỀ AN TOÀN THÔNG TIN
INFORMATION SECURITY OVERVIEW

Khái niệm

- Thông tin: là những gì mang lại hiểu biết về thế giới xung quanh (sự vật, sự kiện, hiện tượng …) và các kiến thức để giải quyết các thông tin.
- Các dạng thông tin: Số, Phi số, Sinh học …
- Thông tin được mã hóa thành nhiều dạng khác nhau để lưu trữ, truyền và xử lý.
- Thông tin luôn mang một ý nghĩa xác định nhưng hình thức thể hiện của thông tin thì mang tính quy ước.
- Lưu trữ: Thông tin được lưu trữ bởi các phương tiện lưu trữ: in, phim, từ tính, quang học.

Khái niệm

- Môi trường thông tin: tự nhiên tiếng nói, nhân tạo sóng âm, sóng âm thanh, điện …
- Dữ liệu: một phần/dạng của thông tin.
- Dữ liệu kỹ thuật số (Dữ liệu số): đòi hỏi được lưu trữ, truyền và xử lý bởi năng lượng điện và đọc được bằng máy. Biểu diễn = bit

Thông tin = Dữ liệu = Dữ liệu số

Khái niệm

- An toàn thông tin (ATTT) là kỹ thuật an toàn cho các hoạt động của các cơ sở hạ tầng thông tin (HTTT) nhằm đảm bảo các tính chất an toàn của thông tin.
- Trong đó bao gồm an toàn phần cứng và phần mềm theo các tiêu chuẩn kỹ thuật do nhà nước hoặc các cơ quan quốc tế ban hành (ISO, Thông tư, quy định …)
- Mục tiêu hướng tới của ATTT là bảo vệ các tài sản thông tin.

Khái niệm

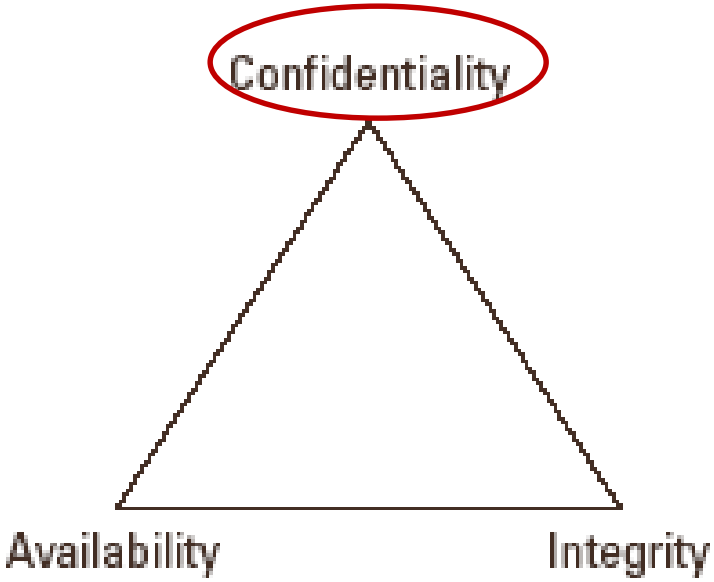
- ISO/IEC 27xxx

An toàn thông tin

- Vào hai thập niên cuối của thế kỷ 20, sự giải thích thuật ngữ *an toàn thông tin* (*information security*) đã có hai sự thay đổi quan trọng.
  - *An toàn máy tính* (*computer security*).
  - *An toàn mạng* (*network securty*)

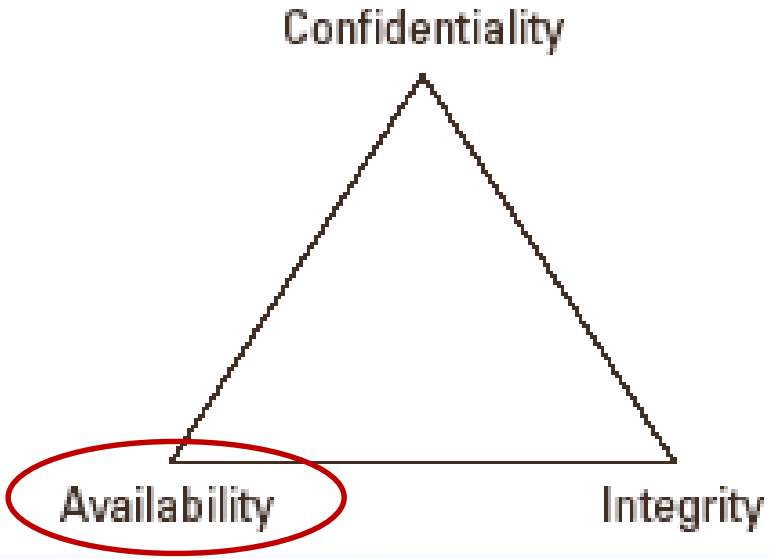
Các muc tiêu chính an toàn thông tin – Bộ ba CIA

- Tính bí mật - người ngoài cuộc không thể đọc dữ liệu ngay cả khi xảy ra rò rỉ thông tin (ứng dụng mã hoá bảo mật).



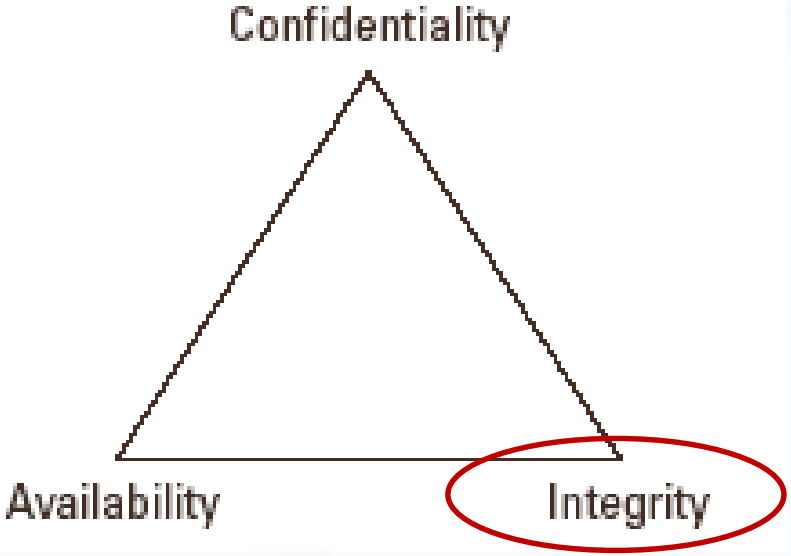
(tiếp)

- Tính sẵn sàng - đây là khả năng nhận được thông tin cần thiết vào thời điểm cần thiết bất kỳ với toàn bộ các thay đổi tại thời điểm này.



(tiếp)

- Tính toàn vẹn - có nghĩa là các dữ liệu tin cậy không bị thay đổi (trong kết quả truyền đi hoặc biến dạng cố ý) từ thời điểm tạo nên đến thời điểm chúng được xem xét.



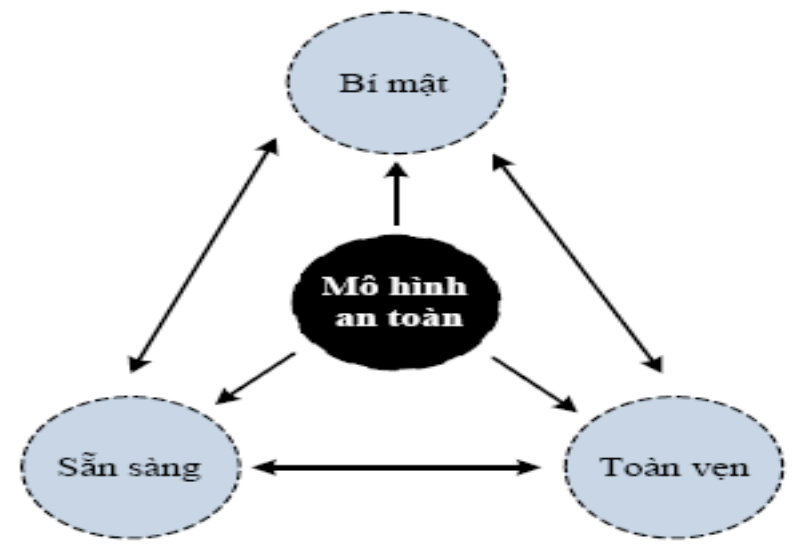
(tiếp)

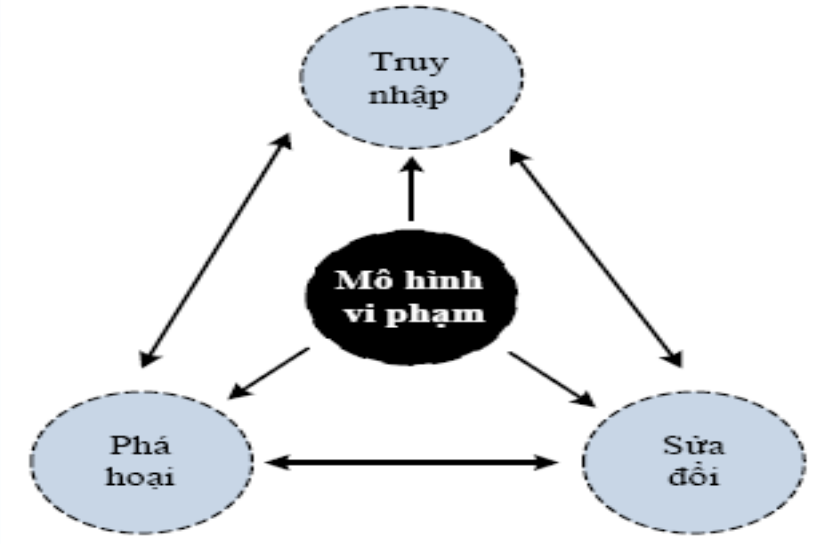
- Các kỹ thuật an toàn phải cố gắng bảo vệ cả 3 mục tiêu này, bởi vì chỉ một trong 3 mục tiêu có yếu điểm thì một hệ thống hoặc mạng sẽ bị xâm phạm.
- Những kẻ vi phạm cũng phát triển một bộ ba cho chúng "bộ ba DAD" để chống lại "bộ ba CIA".

Bộ ba DAD

Mỗi mục tiêu của DAD có nhiệm vụ chống lại một cơ chế được thực hiện trên một mục tiêu của CIA.

- Truy nhập thông tin trái phép (Disclosure).
- Sửa đổi thông tin (Alteration).
- Phá hoại thông tin (Destruction).





Các cơ chế đảm bảo CIA
Tính bí mật

- Đảm bảo tính bí mật của thông tin, tức là thông tin chỉ được phép truy cập (đọc) bởi những đối tượng (người, chương trình máy tính…) được cấp phép.
- Tính bí mật của thông tin có thể đạt được bằng cách giới hạn truy cập về cả mặt vật lý và các cơ chế hoạt động của Hệ thống thông tin.

Các cơ chế đảm bảo CIA
Tính bí mật

- **Cơ chế về bảo vệ can thiệp vật lý vào hệ thống:** ngăn chặn các truy cập trái phép trực tiếp vào hệ thống: máy tính, server, cab … cũng như các sự cố vật lý.
- **Các cơ chế điều khiển truy nhập**: ngăn chặn các đối tượng trái phép truy nhập vào mạng và sửa đổi thông tin.
- **Cơ chế điều khiển quyền người dùng**: ngăn chặn các đối tượng hợp pháp vượt quyền truy nhập thông tin hoặc các đối tượng trái phép xem trộm thông tin.
- **Cơ chế sử dụng Mã hóa**: sử dụng các biện pháp mã hóa để mã hóa các thông tin nhạy cảm.

Các cơ chế đảm bảo CIA
Tính bí mật

- Khóa kín và niêm phong thiết bị, xây dựng hệ thống backup, lưu điện, chống cháy nổ...
- Sử dụng firewall hoặc ACL trên router để ngăn chặn truy cập trái phép.
- Yêu cầu đối tượng cung cấp credential, ví dụ, cặp username + password hay đặc điểm về sinh trắc để xác thực.
- Mã hóa thông tin sử dụng các giao thức và thuật toán mạnh như SSL/TLS, AES, v.v..

Các cơ chế đảm bảo CIA
Tính toàn vẹn

- Tính toàn vẹn bao gồm toàn vẹn dữ liệu (nội dung của thông tin) và toàn vẹn nguồn gốc (nguồn gốc của dữ liệu, thường được gọi là xác thực).
- Các cơ chế toàn vẹn được chia thành 2 lớp: các cơ chế ngăn chặn và các cơ chế phát hiện.

Các cơ chế đảm bảo CIA
Tính toàn vẹn

- Các cơ chế ngăn chặn đảm bảo tính toàn vẹn bằng cách ngăn chặn bất kỳ các truy nhập trái phép để sửa đổi dữ liệu.
- Các cơ chế phát hiện không thực hiện việc ngăn chặn xâm phạm tính toàn vẹn mà chỉ cung cấp các báo cáo về sự toàn vẹn của dữ liệu.

Các cơ chế đảm bảo CIA
Tính toàn vẹn

- Các cơ chế điều khiển truy nhập: ngăn chặn các đối tượng trái phép truy nhập vào mạng và sửa đổi thông tin.
- Điều khiển quyền người dùng: thực hiện việc cấp quyền cho các người dùng trong mạng.
- Mật mã: sử dụng chữ kí số để xác nhận rằng thông tin không bị sửa đổi khi truyền.

Các cơ chế đảm bảo CIA
Tính sẵn sàng

- Tính sẵn sàng là một phương diện rất quan trọng của độ tin cậy của hệ thống.
- Đảm bảo độ sẵn sàng của thông tin, tức là thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn.
- Thực hiện các cơ chế đảm bảo an ninh hệ thống: Back up, Load balancing, Clustering, Redudancy, Failover…

Các cơ chế khác

1. Định danh (Identification):
Người dùng cung cấp danh định (identity)
(Account, Biometric Indentity, Digital identity)
2. Xác thực (Authentication):
Người dùng chứng minh danh định đó là đúng
3. Ủy quyền (Authorization):
Xác định quyền mà người dùng có
4. Kiểm toán (Accounting):
Các hoạt động của người dung
5. Tính không thể chối từ (Non – Repudiation)

.....

Vai trò của Các cơ chế khác

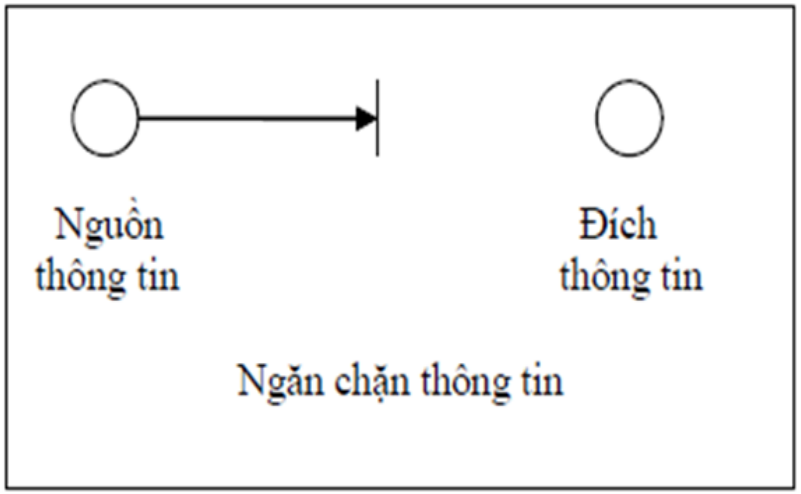
- Cho phép người dùng được xác định đối với các tài nguyên được bảo vệ.
- Cung cấp một cơ chế kiểm soát từ tài nguyên đến đối tượng xác nhận định danh của người dùng.
- Cung cấp quyền quản trị tài nguyên với các cơ chế định rõ người dùng có thể truy nhập tới tài nguyên nào và các hành động có thể thực hiện trên chúng.
- Cung cấp các công cụ bổ sung trong việc ghi nhận các hành động của người dùng hợp lệ trên tài nguyên và kiểm soát chúng.

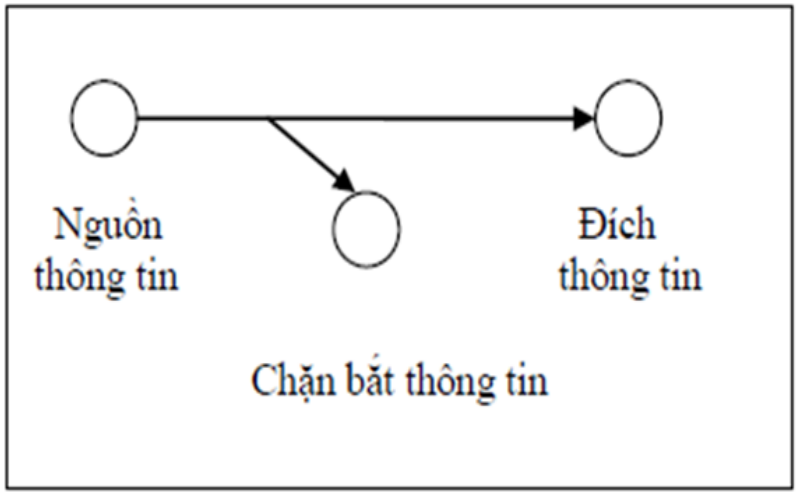
Nhận xét

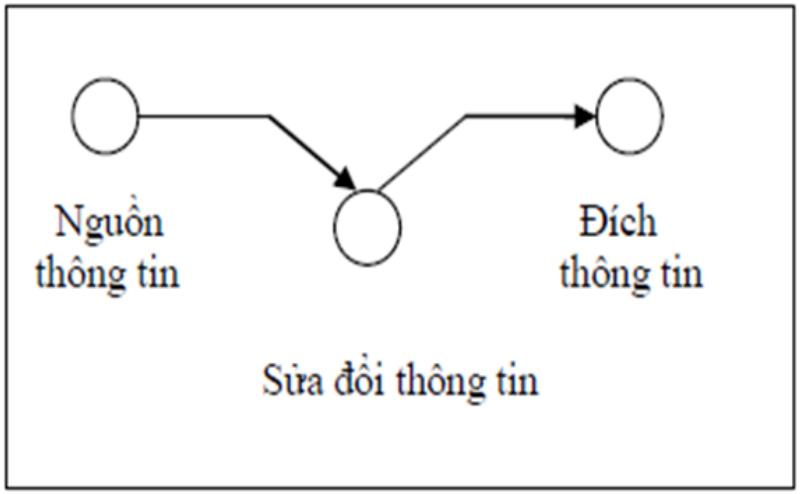
- Không tồn tại một cơ chế duy nhất, để đạt được mục đích an toàn thì các cơ chế khác nhau sẽ được sử dụng.
- Cơ sở của phần lớn các cơ chế an toàn thuộc các phương pháp mật mã.
- Mã hoá hoặc gần tới mã hoá để biến đổi thông tin là các phương pháp phổ biến nhất cho an toàn số liệu.

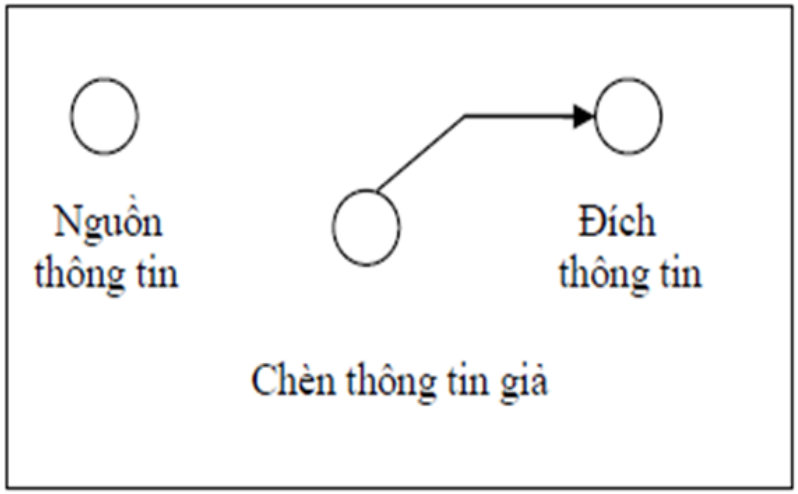
TẤN CÔNG THÔNG TIN TRÊN MẠNG

Các loại tấn công đối với thông tin trên mạng









Các tấn công đối với thông tin trên mạng

- **Tấn công ngăn chặn thông tin (interruption)**

Tài nguyên thông tin bị phá hủy, không sẵn sàng phục vụ hoặc không sử dụng được.

Đây là hình thức tấn công làm mất khả năng sẵn sàng phục vụ của thông tin → ?

- **Tấn công chặn bắt thông tin (interception)**

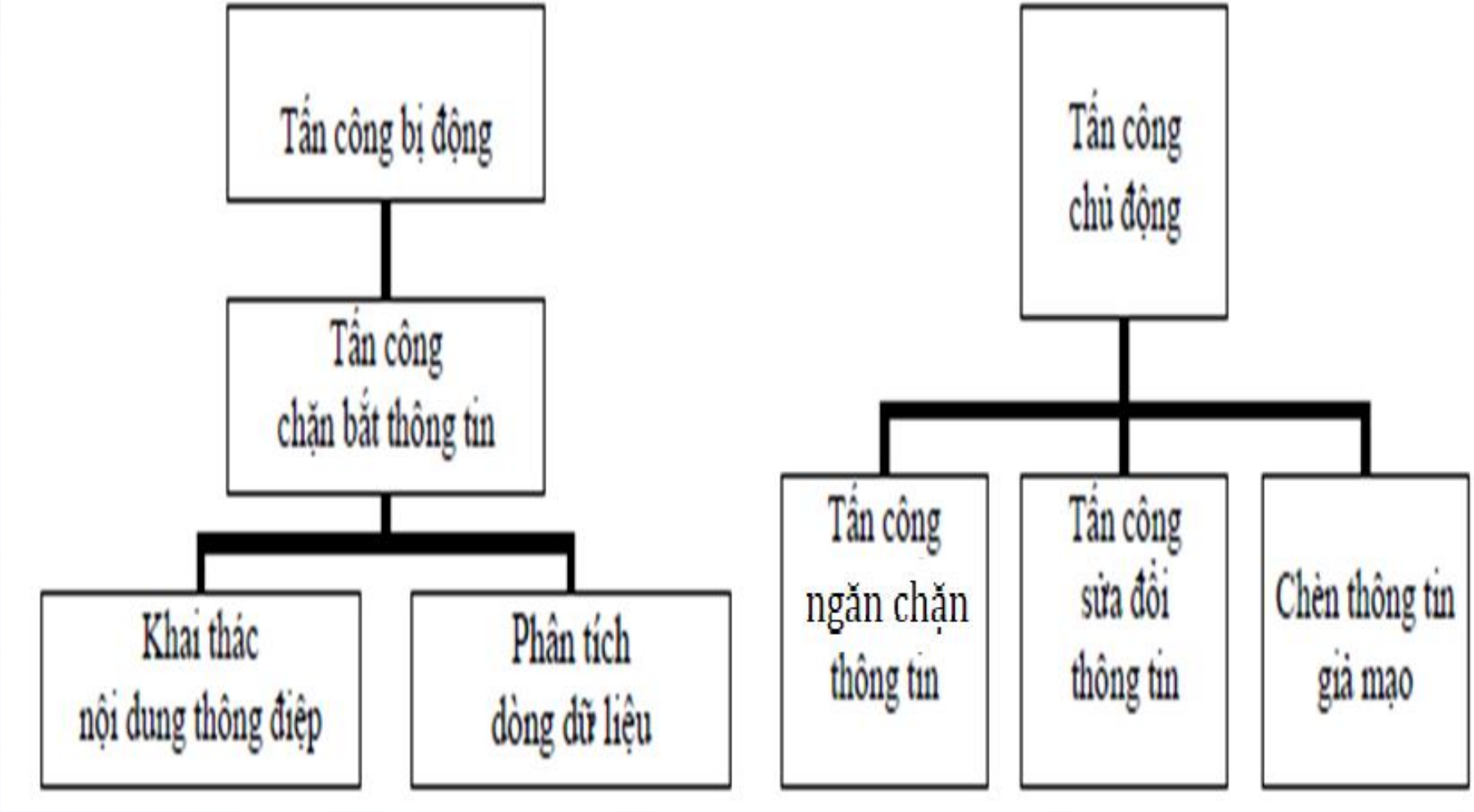
Kẻ tấn công có thể truy nhập tới tài nguyên thông tin.

Đây là hình thức tấn công vào tính bí mật của thông tin.

Các tấn công đối với thông tin trên mạng

- **Tấn công sửa đổi thông tin (Modification)**
  - Kẻ tấn công truy nhập, chỉnh sửa thông tin trên mạng.
  - Đây là hình thức tấn công vào tính toàn vẹn của thông tin.
- **Chèn thông tin giả mạo (Fabrication)**
  - Kẻ tấn công chèn các thông tin và dữ liệu giả vào hệ thống.
  - Đây là hình thức tấn công vào tính

Tấn công bị động (Passive attacks) và chủ động (Active attacks)



TẤN CÔNG BỊ ĐỘNG (PASSIVE ATTACKS)

- Mang đặc trưng chặn bắt thông tin nhằm mục đích phá vỡ tính bí mật của hệ thống
- Đặc điểm: Chỉ thực hiện thao tác thu thập thông tin, không tác động đến các chủ thể trong cuộc đối thoại (đích, nguồn, thông tin)

→ khó phát hiện

- Bao gồm:
  - Khai thác nội dung thông điệp
  - Phân tích dòng dữ liệu.

Nhận xét

- Khó phát hiện
- Thực hiện phòng ngừa
- Giải pháp ?

TẤN CÔNG CHỦ ĐỘNG (ACTIVE ATTACKS)

- Tấn công chủ động: Các phá hoại có liên quan đến việc thay đổi dòng thông tin truyền bằng cách sửa hoặc tạo ra các dòng dữ liệu giả. → tác động đến chủ thể truyền.
- Tác hại: CIA
- Bao gồm
  - Mô phỏng
  - Khôi phục
  - Sửa thông điệp
  - Gây nhiễu trong phục vụ.

TẤN CÔNG CHỦ ĐỘNG (ACTIVE ATTACKS)

- Giả mạo (Masquerade)(Mô phỏng) có nghĩa là sự cố gắng của một đối tượng để đưa chính mình thành đối tượng khác để truyền, nhận thông tin (tạo thông tin giả).
- Dùng lại (Replay) là việc ăn cắp thụ động khối dữ liệu và tiếp sau truyền lặp lại khối dữ liệu đó với mục đích nhận được hiệu ứng trái phép.

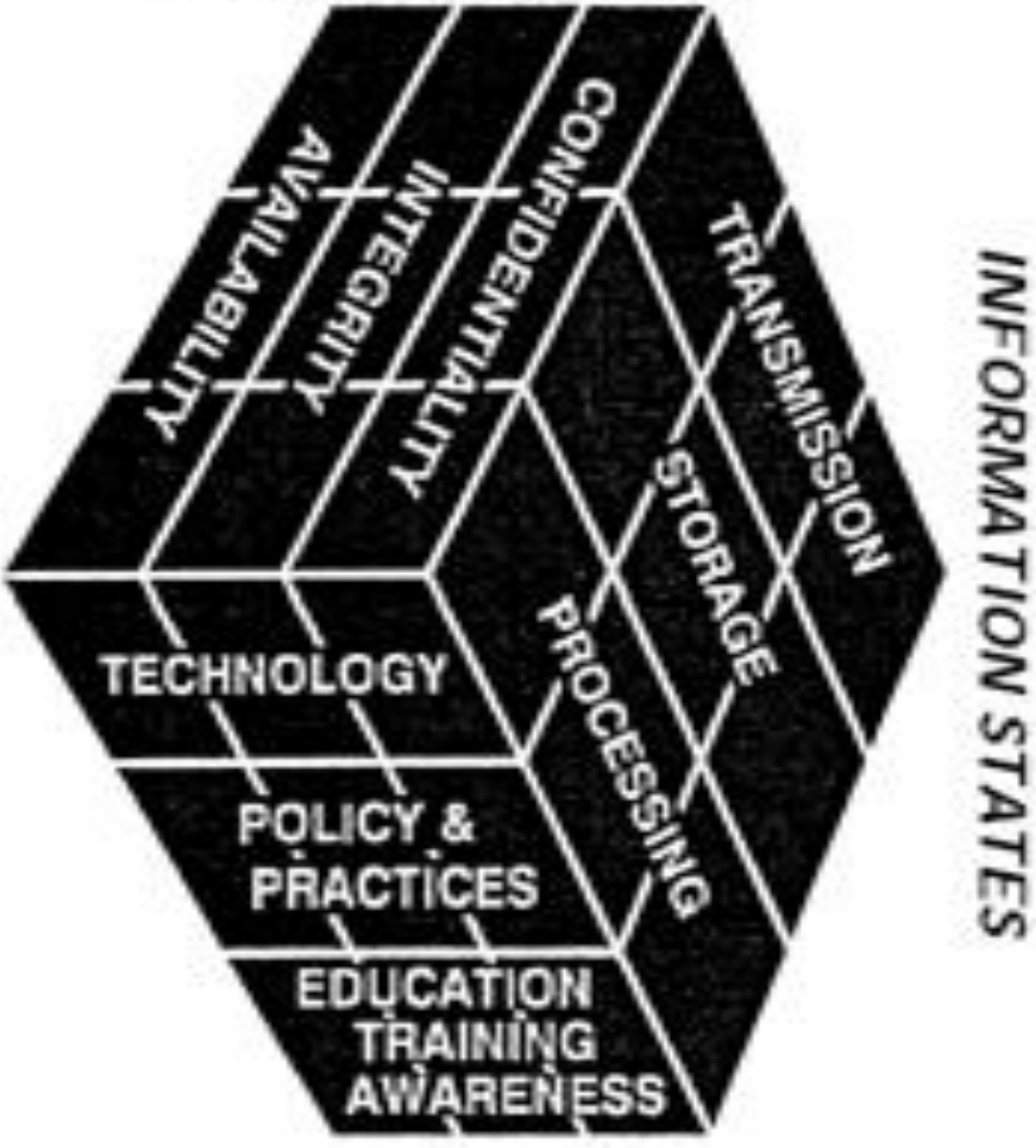
(tiếp)

- Sửa thông điệp (Modification of messages): Biến dạng thông tin bằng cách thay đổi một phần thông tin gốc, thay đổi thứ tự đến của tin tức hoặc là tác động làm trễ nó với mục đích nhận được hiệu ứng trái phép.
- Từ chối dịch vụ (Denial of Service - DoS): (Gây nhiễu trong phục vụ) là tạo ra trở ngại cho các hành động trên tài sản thông tin giữa người dung hợp pháp và tài sản thông tin đó

Nhận xét

- Dễ phát hiện hơn
- Thực hiện phòng ngừa –phát hiện - xử lý
- Giải pháp ?

GIẢI PHÁP ĐẢM BẢO ATTT


CRITICAL INFORMATION CHARACTERISTICS
AVAILABILITY
INTEGRITY
CONFIDENTIALITY
TRANSMISSION
STORAGE
PROCESSING
INFORMATION STATES
TECHNOLOGY
POLICY & PRACTICES
EDUCATION TRAINING AWARENESS
SECURITY MEASURES

Giải pháp đảm bảo an toàn thông tin (tiếp)

Các biện pháp ATTT được phân loại thành 3 lớp như sau, tạo thành chiều thứ 3 của không gian ma trận:

- **Các biện pháp công nghệ (Technology):** Bao hàm tất cả các biện pháp phần cứng, các phần mềm, phần sụn cũng như các kỹ thuật công nghệ liên quan được áp dụng nhằm đảm các yêu cầu an toàn của thông tin trong các trạng thái của nó.

GIẢI PHÁP ĐẢM BẢO ATTT (TIẾP)

- **Các biện pháp về chính sách và tổ chức (Policy & Practices):** Đưa ra các chính sách, quy định, phương thức thực thi.
- Thực tế cho thấy, ATTT không chỉ đơn thuần là vấn đề thuộc phạm trù công nghệ, kỹ thuật. Hệ thống chính sách và kiến trúc tổ chức đóng một vai trò hữu hiệu trong việc đảm bảo an toàn thông tin.

GIẢI PHÁP ĐẢM BẢO ATTT (TIẾP)

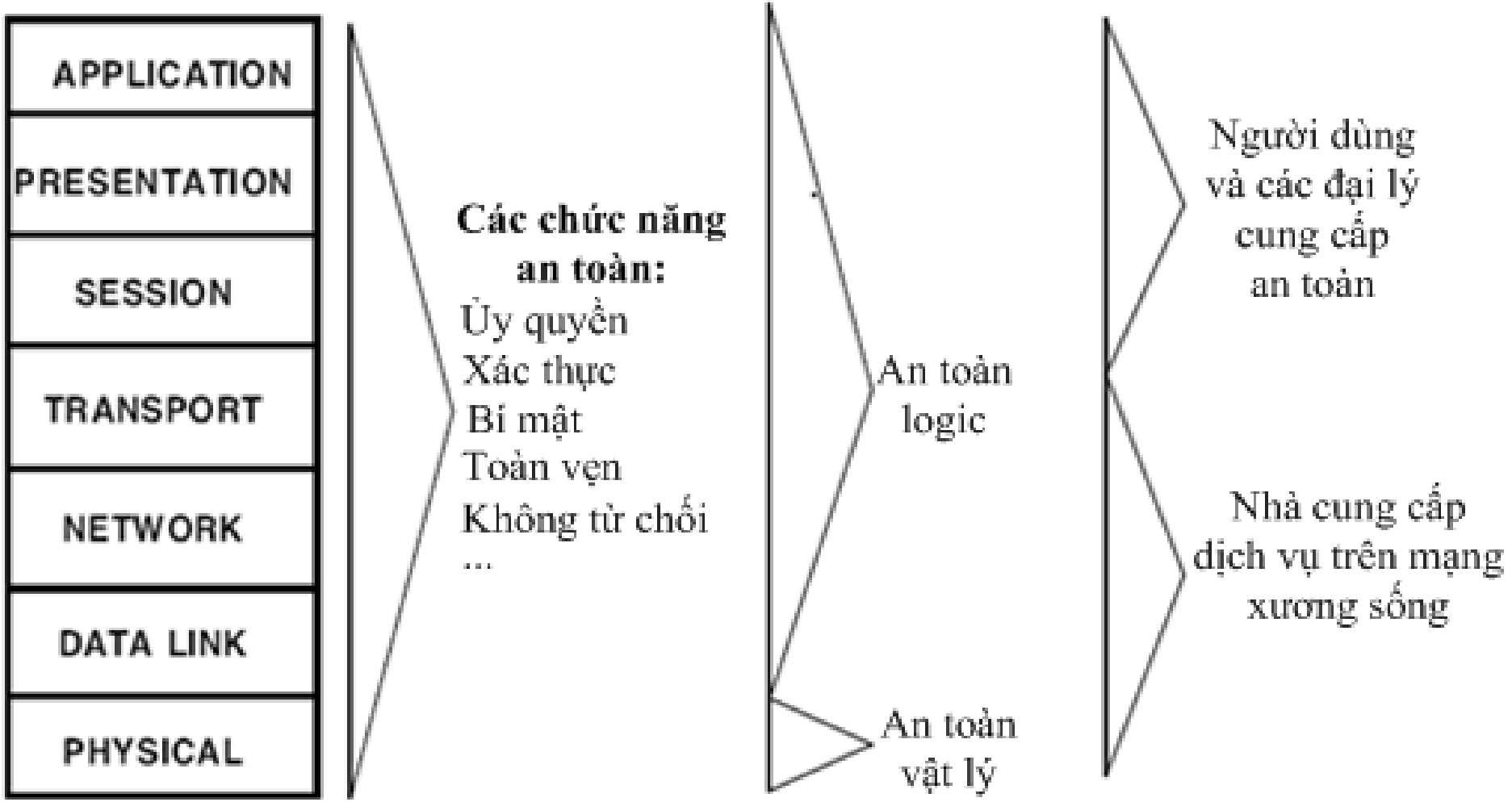
- **Các biện pháp về đào tạo, tập huấn, nâng cao nhận thức (Education, training & Awarenness):** Các biện pháp công nghệ hay các biện pháp về tổ chức thích hợp phải dựa trên các biện pháp đào tạo, tập huấn và tăng cường nhận thức để có thể triển khai đảm bảo an toàn thông tin từ nhiều hướng khác nhau.

GIẢI PHÁP ĐẢM BẢO ATTT (TIẾP)

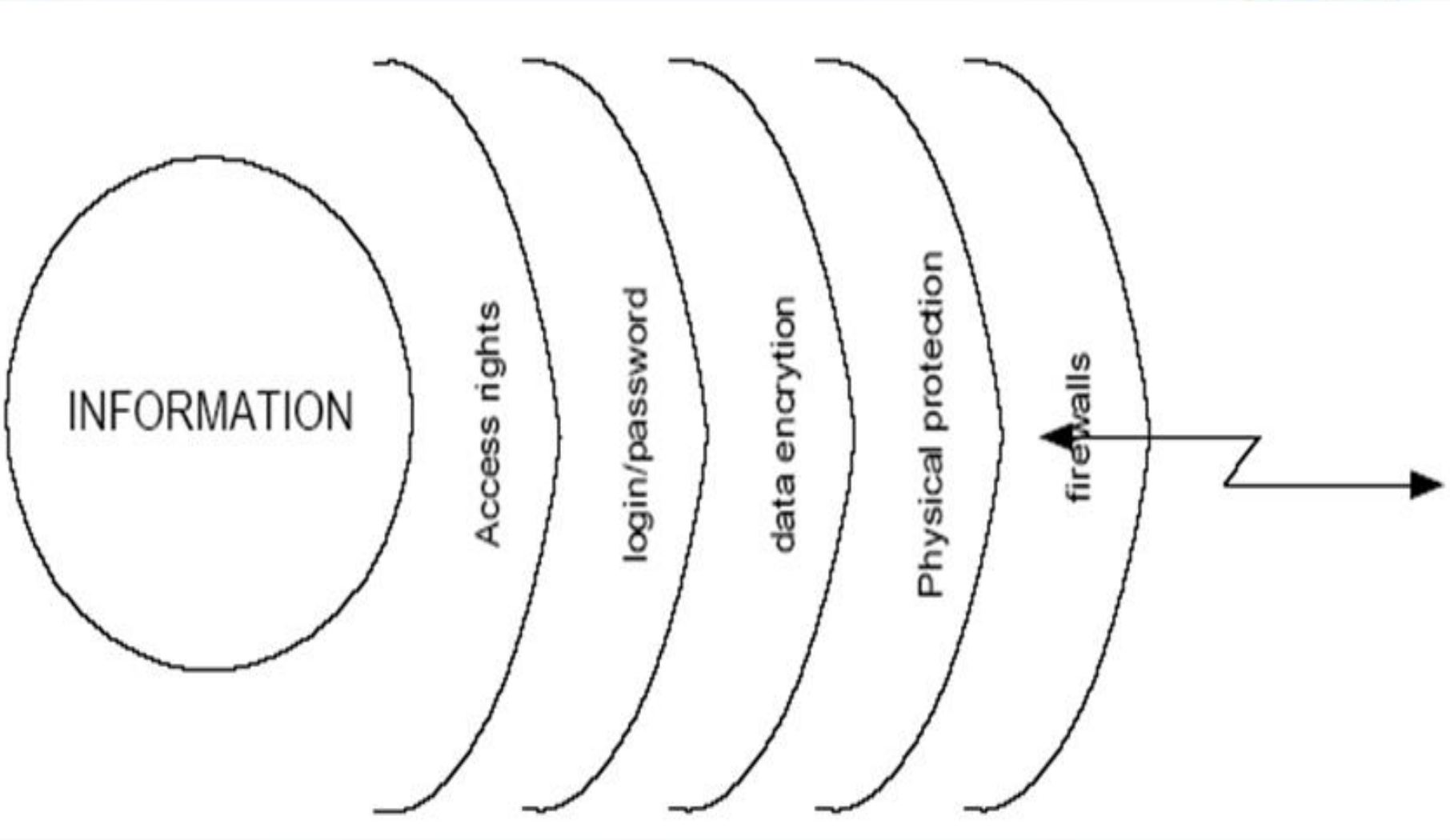
Đứng trên góc độ Vĩ mô:

- Các nhà nghiên cứu và các kỹ sư cũng cần phải hiểu rõ các nguyên lý an toàn hệ thống thông tin, thì mới mong các sản phẩm và hệ thống do họ làm ra đáp ứng được các nhu cầu về an toàn thông tin của cuộc sống hiện tại đặt ra.
- Hợp tác với các quốc gia có kinh nghiệm, kế thừa những thành tựu khoa học của các quốc gia đi trước trong vấn đề đảm bảo ATTT.
- Xây dựng các quy chế phối hợp với các cơ quan tổ chức quốc tế trong ứng phó các sự cố về ATTT.

ATTT và OSI


APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATA LINK
PHYSICAL
Các chức năng an toàn:
Ủy quyền
Xác thực
Bí mật
Toàn vẹn
Không từ chối
...
An toàn logic
An toàn vật lý
Người dùng và các đại lý cung cấp an toàn
Nhà cung cấp dịch vụ trên mạng xương sống

Mô hình thiết kế



Yêu cầu của kỹ thuật an toàn

- Kỹ thuật an toàn (security engineering): xây dựng các hệ thống đảm bảo tin cậy khi đối mặt với các nguy cơ và rủi ro thông tin.
- Kỹ thuật an toàn yêu cầu sự thành thạo nhiều vấn đề chuyên môn, từ mật mã và an toàn mạng tới sự hiểu biết về áp dụng các giải pháp tâm lý, vấn đề tổ chức.

Nhận xét

- Trên thực tế thì không có sự tồn tại một giải pháp an toàn thông tin nào dạng plug and play cho các tổ chức.
- Không có một tài liệu nào có thể lượng giá hết mọi lỗ hổng trong hệ thống và cũng không có nhà sản xuất nào có thể cung cấp thiết bị all in one.

Nội dung cần nắm

1. Trình bày các nguyên tắc ATTT cơ bản ? (nêu, phân tích, ví dụ) CIA.
2. Trình bày các loại phá hoại thông tin.
3. Các yêu cầu khi thiết kế giải pháp ATTT cho doanh nghiệp.
4. Tìm hiểu chuẩn và mô hình ATTT cho ngân hàng. (Key: NIST, ISO 27000, PCI DSS, CSF)

THANK YOU !