Chương I

1

TỔNG QUAN VỀ AN TOÀN HỆ THỐNG THÔNG TIN

GV: Trần Thị Kim Chi

NỘI DUNG

1. Các khái niệm cơ bản về an toàn thông tin
2. Các nguyên tắc nền tảng của an toàn thông tin
3. Các nguy cơ mất an toàn thông tin
4. Tầm quan trọng an toàn thông tin đối với xã hội/doanh nghiệp/cá nhân
5. Các phương pháp đảm bảo an toàn thông tin
6. Các thành phần cần bảo vệ trong một HTTT
7. CÂU HỎI VÀ BÀI TẬP

1 Các khái niệm cơ bản về an toàn thông tin

Data (dữ liệu) và information (thông tin)

Dữ liệu

Baker, Kenneth D.	324917628
Doyle, Joan E.	476193248
Finkle, Clive R.	548429344
Lewis, John C.	551742186
McFerran, Debra R.	409723145

Thông tin

Class Roster

Course: MGT 500 Business Policy Semester: Spring 2010

Section: 2

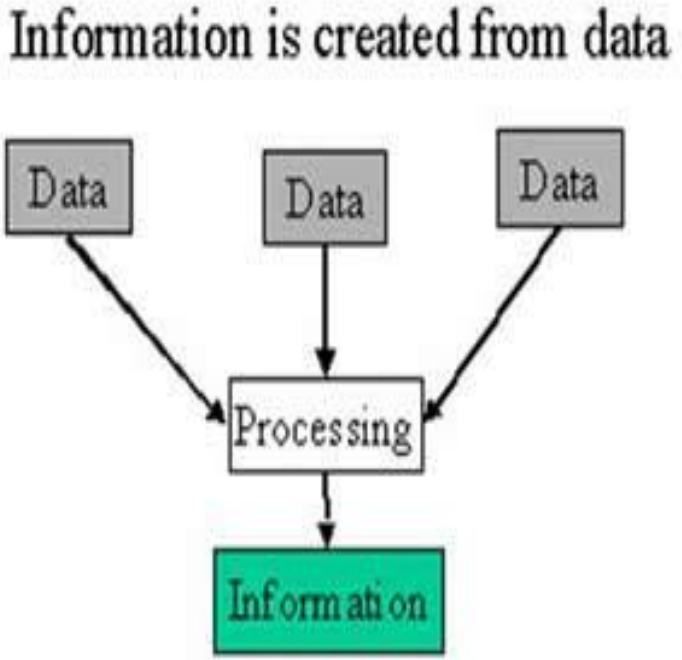
Name	ID	Major	GPA
Baker, Kenneth D.	324917628	MGT	2.9
Doyle, Joan E.	476193248	MKT	3.4
Finkle, Clive R.	548429344	PRM	2.8
Lewis, John C.	551742186	MGT	3.7
McFerran, Debra R.	409723145	IS	2.9
Sisneros, Michael	392416582	ACCT	3.3

Các khái niệm cơ bản về an toàn thông tin

- **Dữ liệu (Data) là gì?**
  - Dữ liệu có thể được định nghĩa như là một tập các sự việc, sự kiện, con số.
    - Ví dụ: họ tên, ngày sinh của một người, trọng lượng, giá cả, chi phí số lượng, tên sản phẩm, mã số thuế,....
  - Dữ liệu là không có ý nghĩa cho đến khi nó được đưa vào một mối liên quan nào đó
  - Dữ liệu có thể được thu thập, xử lý, lưu trữ trong máy tính
  - Dữ liệu mà chưa xử lý được gọi là dữ liệu thô (Raw data),
  - Dữ liệu được trình bày dước dạng: các con số, các từ, hình ảnh, âm, thanh, đa phương tiện, dữ liệu động
- Hãy cho ví dụ một vài dữ liệu

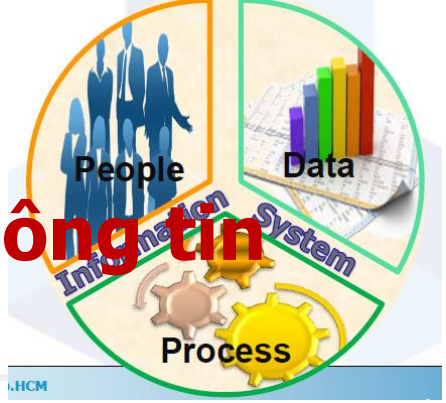
Các khái niệm cơ bản về an toàn thông tin

- **Thông tin (Information) là gì?**
  - Là dữ liệu đã được xử lý, tổ chức, cấu trúc hoặc trình bày trong một ngữ cảnh nhất định để làm cho chúng hữu ích
  - Là dữ liệu đã được xử lý theo cách có ý ghĩa đối với người được nhận nó.
- **Cho ví dụ vài thông tin**

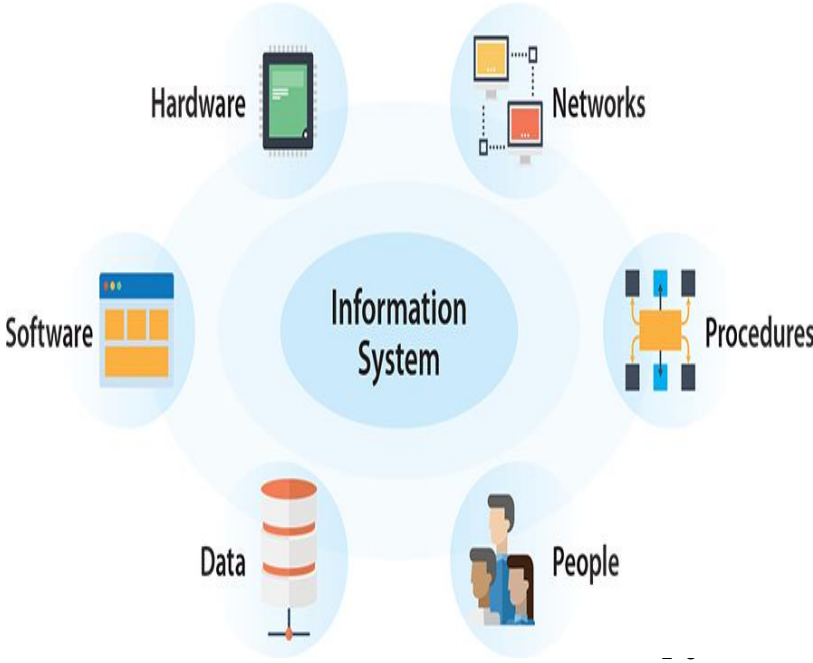


DỮ LIỆU (DATA) → **XỬ LÝ** → **THÔNG TIN (INFORMATION)**

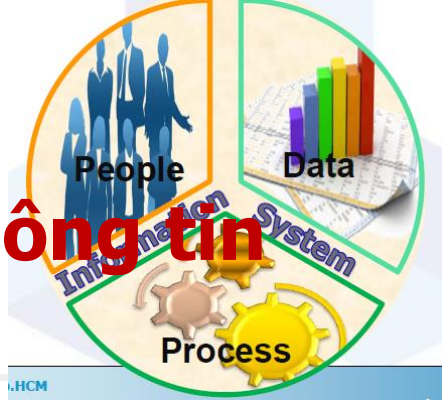
Các khái niệm cơ bản về an toàn thông tin



- ***Hệ thống thông tin (Information Systems)***
  - Là một hệ thống gồm con người, dữ liệu và những hoạt động xử lý dữ liệu và thông tin trong một tổ chức.
- **Tài sản của hệ thống thông tin bao gồm:**
  - ✓ Phần cứng
  - ✓ Phần mềm
  - ✓ Dữ liệu
  - ✓ Mạng
  - ✓ Môi trường làm việc
  - ✓ Con người



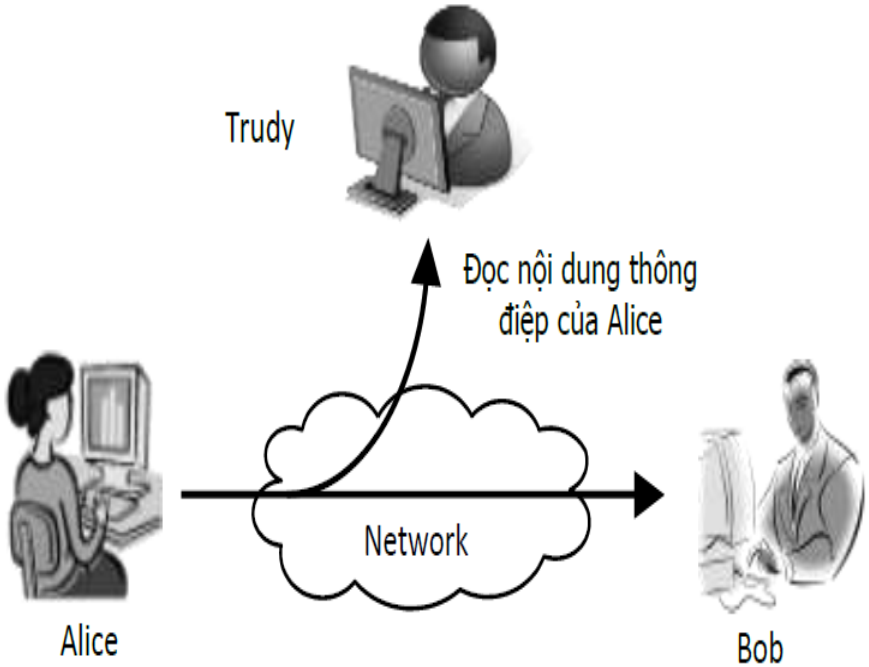
Các khái niệm cơ bản về an toàn thông tin



Hệ thống thông tin (Information Systems)

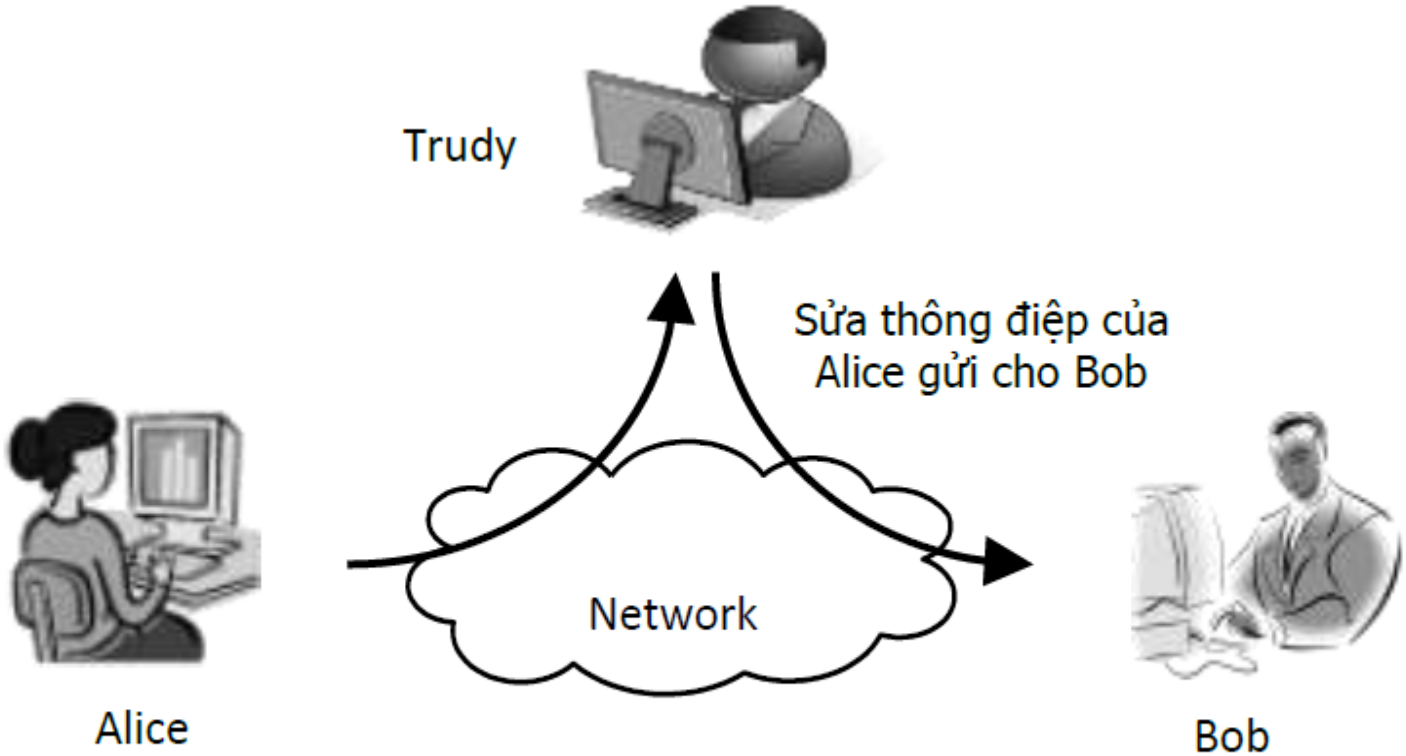
- Hãy cho ví dụ một hệ thống thông tin của một doanh nghiệp mà bạn biết
  - Hệ thống thông tin đó là gì
  - Mục tiêu của hệ thống thông tin đó
  - Các thông tin dữ liệu nào có trong hệ thống thông tin
  - Những ai được truy xuất những thông tin dữ liệu/chức năng nào

An Toàn thông tin là gì? (Information Security)



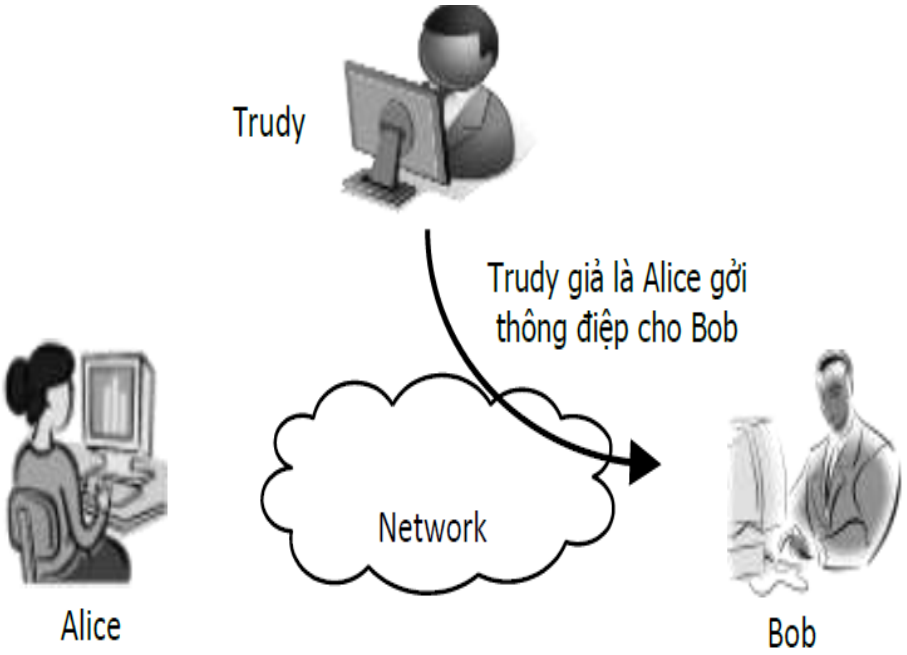
Hình 1-1. Xem trộm thông điệp

An Toàn thông tin là gì? (Information Security)



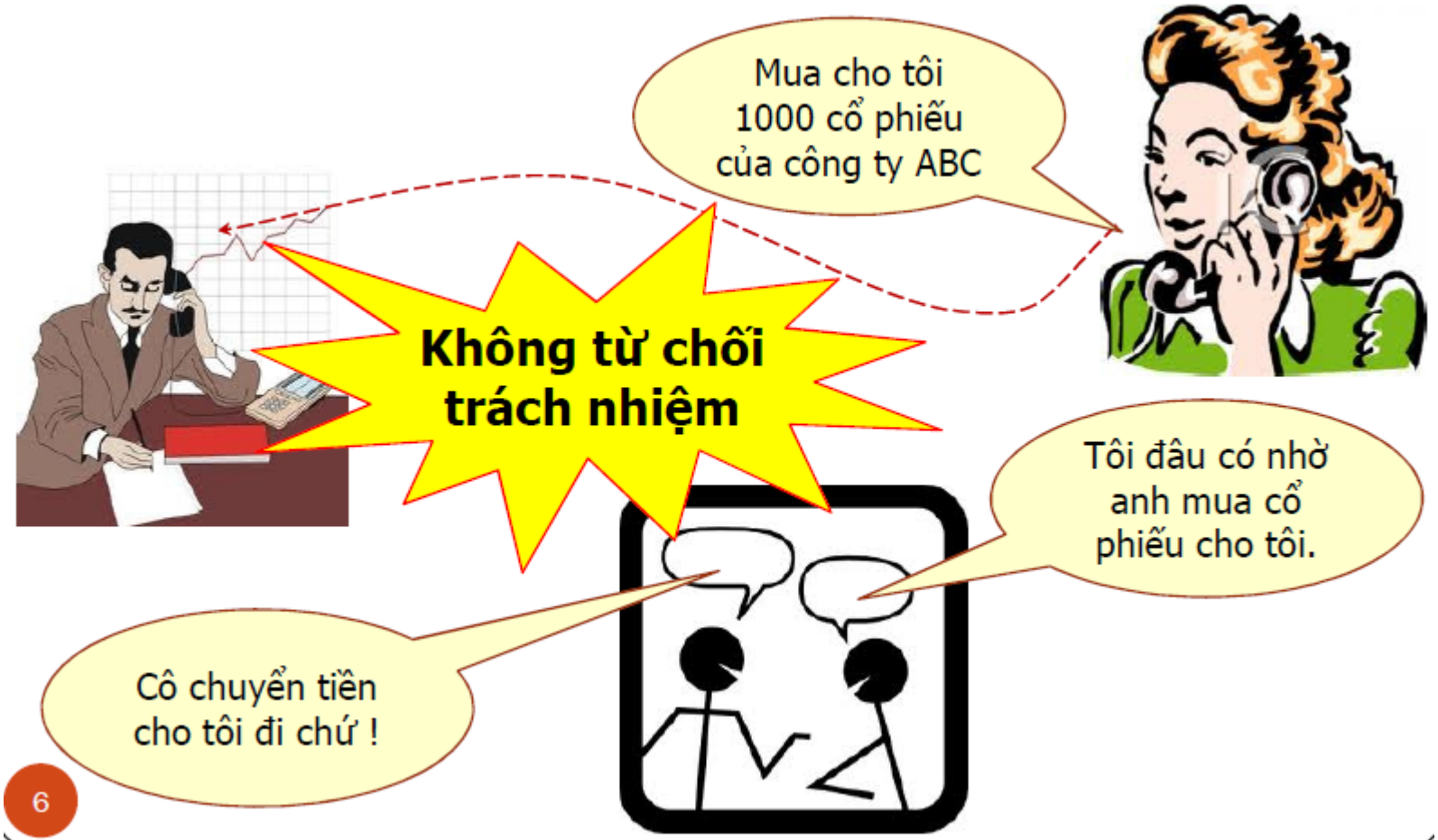
Hình 1-2. Sửa thông điệp

An Toàn thông tin là gì? (Information Security)



Hình 1-3. Mạo danh

An Toàn thông tin là gì? (Information Security)



An Toàn thông tin là gì? (Information Security)

- Là hành động ngăn cản, phòng ngừa sự sử dụng, truy cập, tiết lộ, chia sẻ, phát tán, ghi lại hoặc phá hủy thông tin chưa có sự cho phép.
- Là tập các quy trình và công cụ được thiết kế và triển khai để bảo vệ các thông tin nhạy cảm của doanh nghiệp từ sự truy cập, hiệu chỉnh, phá hủy không hợp pháp

Tại sao cần An Toàn thông tin (Information Security)

- **Thông tin là một tài sản, giống như các tài sản quan trọng khác của doanh nghiệp, có giá trị đối với tổ chức và cần được bảo vệ một cách phù hợp** (BS ISO 27002:2005)

→ Nếu thông tin của tổ chức lọt vào tay những những người không có thẩm quyền hoặc không hợp pháp thì dẫn đến những hậu quả rất rất nghiêm trọng

→Vì thế, bảo vệ thông tin trở thành một yêu cầu không thể thiếu trong mọi hoạt động nói chung và hoạt động điện tử nói riêng. An toàn thông tin trong thời đại số là quan trọng hơn bao giờ hết

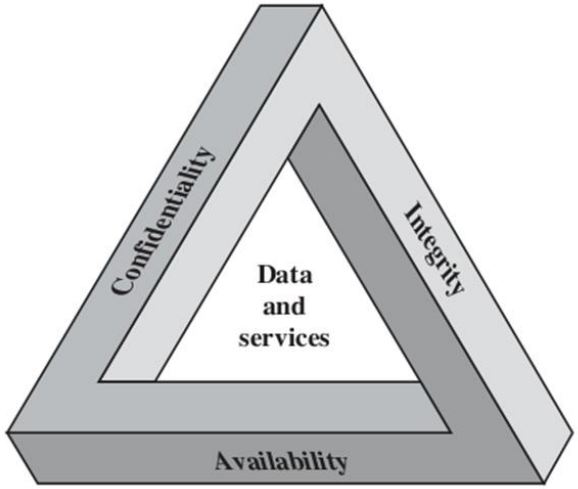
Đảm bảo an toàn thông tin là gì?

- **Đảm bảo ATTT** là đảm bảo an toàn kỹ thuật cho hoạt động của các cơ sở HTTT, trong đó bao gồm đảm bảo an toàn cho cả phần cứng và phần mềm hoạt động theo các tiêu chuẩn kỹ thuật do nhà nước ban hành; ngăn ngừa khả năng lợi dụng mạng và các cơ sở HTTT để thực hiện các hành vi trái phép; đảm bảo các tính chất bí mật, toàn vẹn, sẵn sàng của thông tin trong lưu trữ, xử lý và truyền dẫn trên mạng.

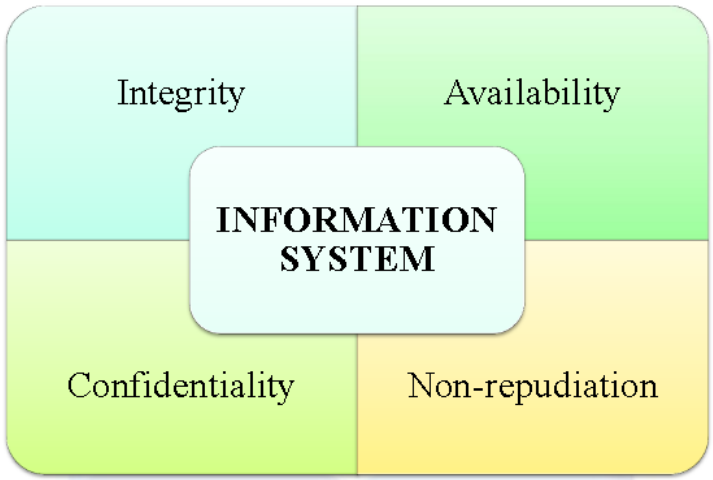
Các nguyên tắc nền tảng của an toàn thông tin (CIA)

Các tính chất cần thiết để một hệ thống đảm bảo an toàn thông tin

- ***Tính bảo mật* (Confidentiality),**
- ***Tính toàn vẹn* (Integrity) và**
- ***Tính sẵn dùng* (Availability)**
- ***Tính chống thoái thác* (Non-repulation)**
- ***Tính xác thực* (Authenticity)**



Tam giác bảo mật CIA (CIA triad).



Các nguyên tắc nền tảng của an toàn thông tin

Tính bí mật (Confidentiality):

- Là nguyên tắc đảm bảo kiểm soát truy cập thông tin, bảo vệ dữ liệu/thông tin không bị lộ ra ngoài một cách trái phép.
- **Thông tin chỉ được phép truy cập bởi những đối tượng** (người, chương trình máy tính…) **được cấp phép.**
- Ví dụ:
  - Trong hệ thống quản lý sinh viên, một sinh viên được phép xem thông tin kết quả học tập của mình nhưng không được phép xem kết quả học tập của sinh viên khác.
  - Trong hệ thống ngân hàng, một khách hàng được phép xem thông tin số dư tài khoản của mình nhưng không được phép xem thông tin của khách hàng khác

Các nguyên tắc nền tảng của an toàn thông tin

Tính toàn vẹn (Integrity):

- Là sự đảm bảo dữ liệu là đáng tin cậy và chính xác.
- **Thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được phép và phải đảm bảo rằng thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi**.
- Ví dụ:
  - Trong hệ thống quản lý sinh viên, không cho phép sinh viên được phép tự thay đổi thông tin kết quả học tập của mình.
  - Trong hệ thống ngân hàng, không cho phép khách hàng tự thay đổi thông tin số dư của tài khoản của mình.

Các nguyên tắc nền tảng của an toàn thông tin

Tính toàn vẹn (Integrity):

- Có ba mục đích chính của việc đảm bảo tính toàn vẹn:
  - Ngăn cản sự làm biến dạng nội dung thông tin của những người sử dụng không được phép.
  - Ngăn cản sự làm biến dạng nội dung thông tin không được phép hoặc không chủ tâm của những người sử dụng được phép.
  - Duy trì sự toàn vẹn dữ liệu cả trong nội bộ và bên ngoài.

Các nguyên tắc nền tảng của an toàn thông tin

Tính sẵn sàng (Availability):

- Là sự đảm bảo liên tục và mức độ đáp ứng kịp thời của hệ thống khi có yêu cầu truy cập dữ liệu hoặc thao tác từ người dùng.
- **Đảm bảo thông tin/dịch vụ luôn sẵn sàng khi những người dùng hoặc ứng dụng được ủy quyền yêu cầu**
- Ví dụ:
  - Trong hệ thống quản lý sinh viên, cần đảm bảo rằng sinh viên có thể truy vấn thông tin kết quả học tập của mình bất cứ lúc nào.
  - Một server chỉ bị ngưng hoạt động hay ngừng cung cấp dịch vụ trong vòng 5 phút trên một năm thì độ sẵn sàng của nó là 99,999%.

Các nguyên tắc nền tảng của an toàn thông tin

- ***Tính chống thoái thác (Non-repudiation)***: Khả năng ngăn chặn việc từ chối một hành vi đã làm.
  - Ví dụ: Trong hệ thống quản lý sinh viên, có khả năng cung cấp bằng chứng để chứng minh một hành vi sinh viên đã làm, như đăng ký học phần, hủy học phần.

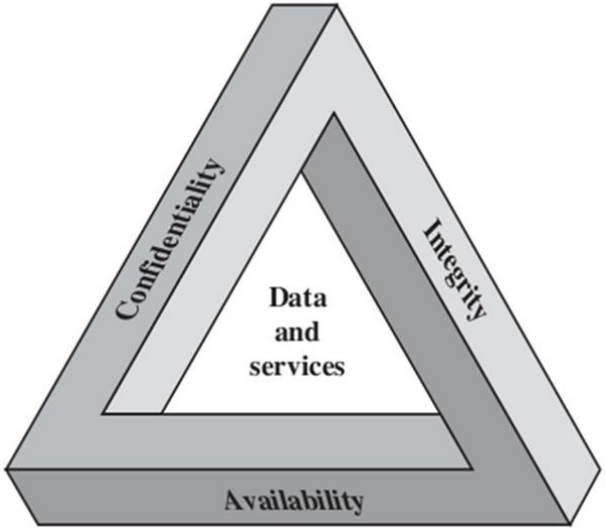
Các nguyên tắc nền tảng của an toàn thông tin

Tính xác thực (Authenticity):

- Việc xác thực nguồn gốc của thông tin trong hệ thống (thuộc sở hữu của đối tượng nào) để đảm bảo thông tin đến từ một nguồn đáng tin cậy
  - **Ví dụ:** Trong hệ thống ngân hàng, có khả năng cung cấp bằng chứng để chứng minh một hành vi khách hàng đã thực hiện và người thực hiện đó có hợp pháp không, như giao dịch thanh toán, giao dịch chuyển khoản....

Các nguyên tắc nền tảng của an toàn thông tin

Mối tương quan giữa **Confidentiality - Integrity – Availability**



$$X\$ = C + I + A$$

Các nguyên tắc nền tảng của an toàn thông tin

Mối tương quan giữa **Confidentiality - Integrity – Availability**

- Bộ ba C, I, A này là những tiêu chí quan trọng trong quá trình phân tích, dự trù kinh phí, thời gian xây dựng hệ thống đảm bảo an toàn thông tin. Các tiêu chí này có mối tương quan như sau:

$$X\$=C+I+A$$

- X$ là kinh phí cho việc xây dựng và phát triển hệ thống C, I, A là thuộc tính của tam giác. Theo toán học, với mỗi X$ không đổi, việc tăng chỉ số C sẽ làm giảm I và A và ngược lại.

Các nguy cơ mất ATTT

- ***Cơ sở hạ tầng mạng***: Cơ sở hạ tầng không đồng bộ, không đảm bảo yêu cầu thông tin được truyền trong hệ thống an toàn và thông suốt.
- ***Thông tin*:** Dữ liệu chưa được mô hình hóa và chuẩn hóa theo tiêu chuẩn về mặt tổ chức và mặt kỹ thuật. Yếu tố pháp lý chưa được trú trọng trong truyền đưa các dữ liệu trên mạng, nghĩa là các dữ liệu được truyền đi trên mạng phải đảm bảo tính hợp pháp về mặt tổ chức và mặt kỹ thuật.

Các nguy cơ mất ATTT

- ***Công nghệ***: Chưa chuẩn hóa cho các loại công nghệ, mô hình kiến trúc tham chiếu nhằm đảm bảo cho tính tương hợp, tính sử dụng lại được, tính mở, an ninh, mở rộng theo phạm vi, tính riêng tư vào trong HTTT.
- ***Con người*:** Sự hiểu biết của những người trực tiếp quản lý, vận hành các HTTT, xây dựng và phát triển hệ thống phần mềm, hệ thống thông tin còn chưa đồng đều và chưa theo quy chuẩn của các cơ quan tổ chức đó.

Các nguy cơ mất ATTT

Quy trình, quản lý:

- Chưa chuẩn hóa qui trình nghiệp vụ trong vận hành HTTT.
- Chưa chuẩn hóa các thủ tục hành chính, các qui định pháp lý trong việc đảm bảo ATTT.
- Tổ chức quản lý thay đổi hệ thống, ứng dụng chưa đúng cách, chưa chuẩn hóa và có chế tài mang tính bắt buộc thực hiện.
- Như vậy để đảm bảo ATTT thì các cơ quan tổ chức phải làm tốt và hạn chế tối đa 5 yếu tố trên.

An toàn thông tin đối với một tổ chức

ATTT thực hiện 4 chức năng quan trọng cho một tổ chức

- Bảo vệ được các chức năng nhiệm vụ của một tổ chức
  - Hoạt động của tổ chức không gián đoạn
  - Không mất chi phí để phục hồi hoạt động của tổ chức
- Có được các hoạt động an toàn trên các ứng dụng của tổ chức
  - Hoạt động của tổ chức hiện đại cần có và vận hành các ứng dụng tích hợp
- Bảo vệ được dữ liệu mà tổ chức đã thu thập và sử dụng
  - Không có dữ liệu, tổ chức sẽ mất các hồ sơ giao dịch hoặc khả năng cung cấp dịch vụ cho khách hàng
- Bảo vệ được tài sản công nghệ của tổ chưc
  - Để thực hiện hiệu quả, các tổ chức phải sử dụng các dịch vụ cơ sở hạ tầng an toàn phù hợp với quy mô và phạm vi của tổ chức. Khi một tổ chức phát triển, nó phải phát triển các dịch vụ bảo mật bổ sung.

Tầm quan trọng an toàn thông tin đối với xã hội/doanh nghiệp/cá nhân

- Quản lý và bảo mật thông tin nhân sự trong tổ chức cần được ưu tiên hàng đầu. Nguồn nhân lực chính là tài sản quý giá đối với mọi doanh nghiệp. Thông tin của nhân viên về chức vụ phòng ban, lương thưởng, nhiệm vụ đảm nhận,... có liên quan mật thiết đến các chiến lược của một doanh nghiệp.
- Do đó, việc để lọt những thông tin cá nhân của nhân viên và dữ liệu liên quan đến quản lý nhân sự cho đối tượng bên ngoài biết được sẽ là một bất lợi vô cùng lớn.

Hậu quả khi thông tin của nhân viên bị tiết lộ ra bên ngoài

- Tin tặc có thể đem những thông tin như họ tên, địa chỉ nơi ở, email, số điện thoại… bán lại cho các doanh nghiệp khác sử dụng với mục đích tiếp thị.
- Cá nhân bị lộ thông tin có thể nhận hàng tá cuộc gọi, email, tin nhắn quảng cáo mỗi ngày, gây ra nhiều phiền nhiễu trong cuộc sống. Thậm chí, kẻ gian có thể lợi dụng những dữ liệu thu thập được để lừa đảo.
- Các thông tin liên quan đến tài khoản ngân hàng bị rò rỉ có thể gây thất thoát tài sản của cá nhân của nhân viên nếu không có biện pháp xử lý kịp thời. Bên cạnh đó, việc thông tin cá nhân bị tiết lộ cũng gây ra hoang mang, lo lắng khiến nhân viên mất niềm tin vào doanh nghiệp.

Hậu quả khi thông tin của nhân viên bị tiết lộ ra bên ngoài

- Nếu thông tin của nhân viên rơi vào tay của đối thủ, doanh nghiệp sẽ đứng trước nguy cơ khủng hoảng nội bộ nghiêm trọng.
- Những thông tin quan trọng như chức vụ của nhân viên, các nhiệm vụ đã và đang đảm nhận và chế độ lương thưởng,... có thể bị các nhà tuyển dụng bên ngoài lợi dụng để chèo kéo nhân viên với vị trí tốt hơn, mức lương cao và phúc lợi tốt hơn.
- Doanh nghiệp có thể bị mất đi những nhân viên chủ lực, tài giỏi. Đánh mất nhân sự vào tay đối thủ sẽ gây ra sự xáo trộn trong bộ máy tổ chức, ảnh hưởng rất lớn đến các hoạt động và hiệu quả kinh doanh.
- Nếu đối thủ nắm trong tay những thông tin về sơ đồ tổ chức thì sẽ dễ dàng nắm được quy trình vận hành cũng như những ý định chiến lược của doanh nghiệp. Từ đó có những hành động gây bất lợi đến công ty.

Một số lưu ý giúp doanh nghiệp bảo mật dữ liệu một cách hiệu quả

- Lên kế hoạch đồng bộ hóa và sao lưu dữ liệu một cách thường xuyên với nền tảng lưu trữ uy tín, nhất là sau khi có sự thay đổi và cập nhật mới nhân sự. Luôn có kịch bản ứng phó kịp thời khi sự cố xảy ra, tránh mất dữ liệu.
- Thiết lập một hệ thống mạng nội bộ an toàn bằng cách sử dụng chương trình, phần mềm hỗ trợ tính năng bảo mật cao. Nếu được, doanh nghiệp nên có chuyên viên có kiến thức về an ninh, bảo mật dữ liệu của doanh nghiệp chịu trách nhiệm về giám sát việc thực hiện các biện pháp an ninh, các quy trình đảm bảo an toàn dữ liệu.

Một số lưu ý giúp doanh nghiệp bảo mật dữ liệu một cách hiệu quả

- **Bảo mật hệ thống thiết bị làm việc bằng cách:** Sử dụng phần mềm mã hóa dữ liệu; Cài đặt Phần mềm Anti-Virus có bản quyền và bật đầy đủ tính năng; Luôn cập nhật những phiên bản hệ điều hành mới nhất.
- Xây dựng chính sách bảo mật rõ ràng theo từng cấp bậc, chức vụ.
- **Phân quyền truy cập vào hệ thống dữ liệu:** Chỉ Ban lãnh đạo và phòng ban có liên quan mới xem và thao tác với các dữ liệu liên quan đến thông tin về nhân sự.
- Nâng cao nhận thức của nhân viên về bảo mật thông tin cá nhân cũng như của doanh nghiệp. Có những tài liệu hướng dẫn về kỹ thuật cũng như lưu ý, hỗ trợ nhân viên của mình trong việc bảo vệ thông dữ liệu.

Thực trạng mất an toàn thông tin tại Việt Nam hiện nay

1. Covid-19 làm gia tăng các sự cố tấn công mạng
2. Tấn công giao dịch ngân hàng gây thiệt hại hàng trăm tỷ đồng
3. Tấn công chuỗi cung ứng trở thành xu hướng mới của tấn công mạng
4. Năm 2021, an ninh mạng toàn cầu diễn biến phức tạp theo đại dịch

Những nguy cơ mất an toàn thông tin và giải pháp (update 2021) (securitybox.vn)

Nguyên nhân mất an toàn thông tin tại Việt Nam hiện nay

1. Nhận thức an ninh mạng chưa tốt
2. Không phân quyền rõ ràng
3. Lỗ hổng bảo mật tồn tại trên các phần mềm
4. Lỗ hổng bảo mật trong chính hệ thống

Những nguy cơ mất an toàn thông tin và giải pháp (update 2021) (securitybox.vn)

Giải pháp để đảm bảo an toàn thông tin

Một số giải pháp (trình bày trong môn này)

- Chính sách ATTT
- Kiểm soát truy cập
- Mật mã học
- Duy trì an toàn thông tin
- Tuân thủ các quy định pháp luật

Các phương pháp đảm bảo an toàn thông tin

- **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.

Các phương pháp đảm bảo an toàn thông tin

- **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.

Các phương pháp đảm bảo an toàn thông tin

Các biện pháp về đào tạo, tập huấn, nâng cao nhận thức (Education, training & Awarenness):

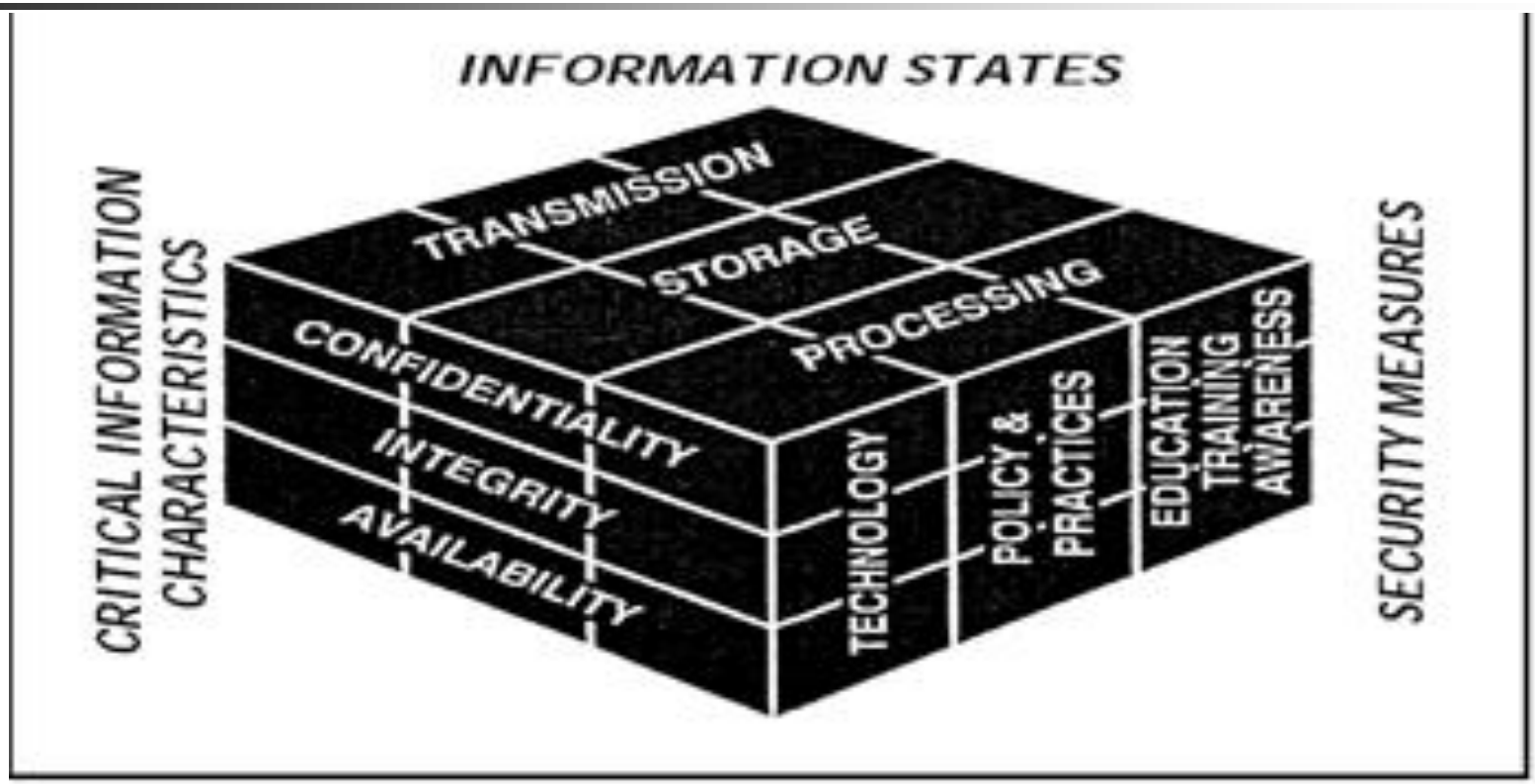
- Các biện pháp công nghệ hay các biện pháp về tổ chức thích hợp phải dựa trên các biện pháp đào tạo, tập huấn và tăng cường nhận thức để có thể triển khai đảm bảo an toàn thông tin từ nhiều hướng khác nhau.
- Các nhà nghiên cứu và các kỹ sư cũng cần phải hiểu rõ các nguyên lý an toàn hệ thống thông 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.

Các phương pháp đảm bảo an toàn thông tin

Biện pháp hợp tác quốc tế

- 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.

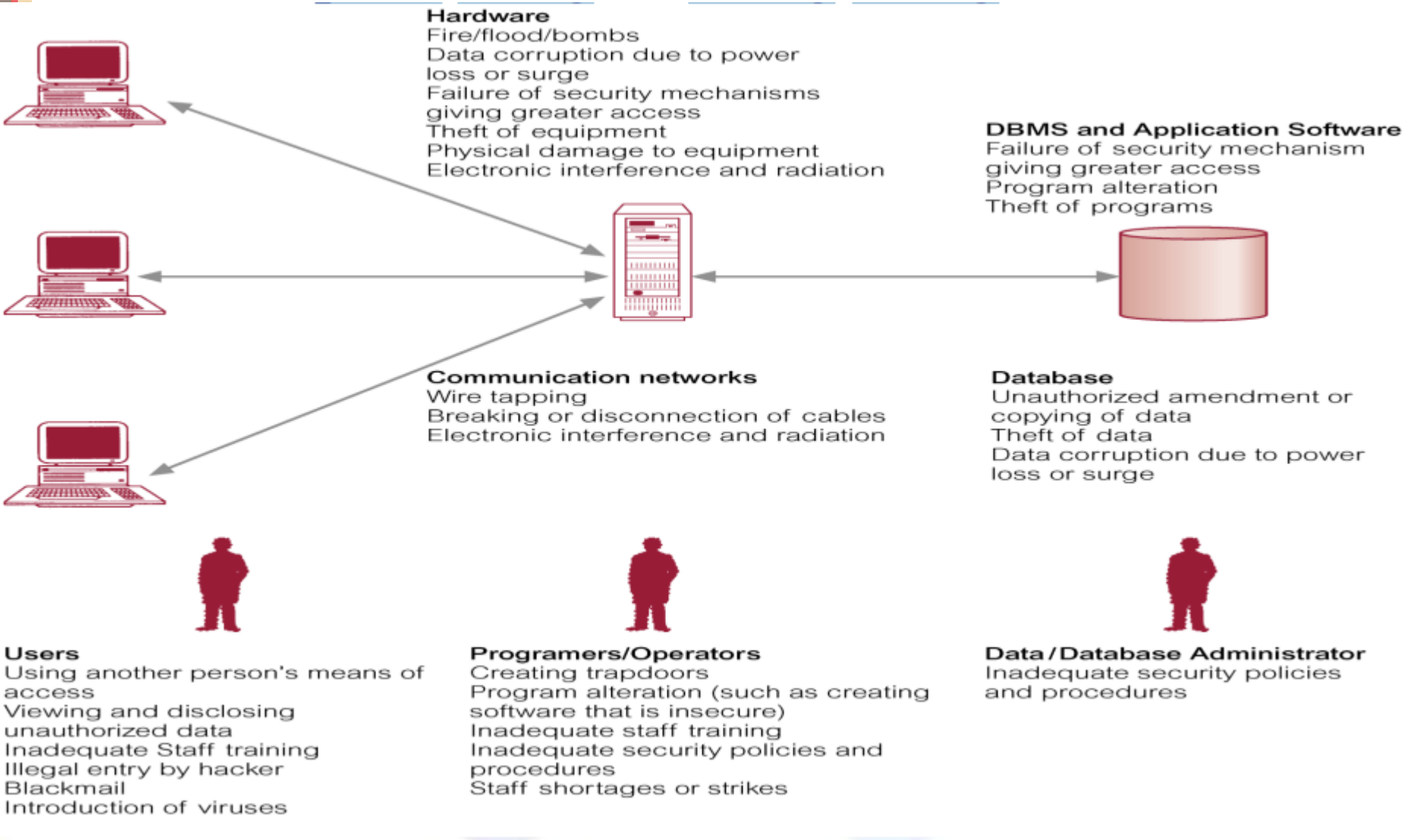
Các phương pháp đảm bảo an toàn thông tin



Hình 2

Mô hình tổng quát về an toàn thông tin

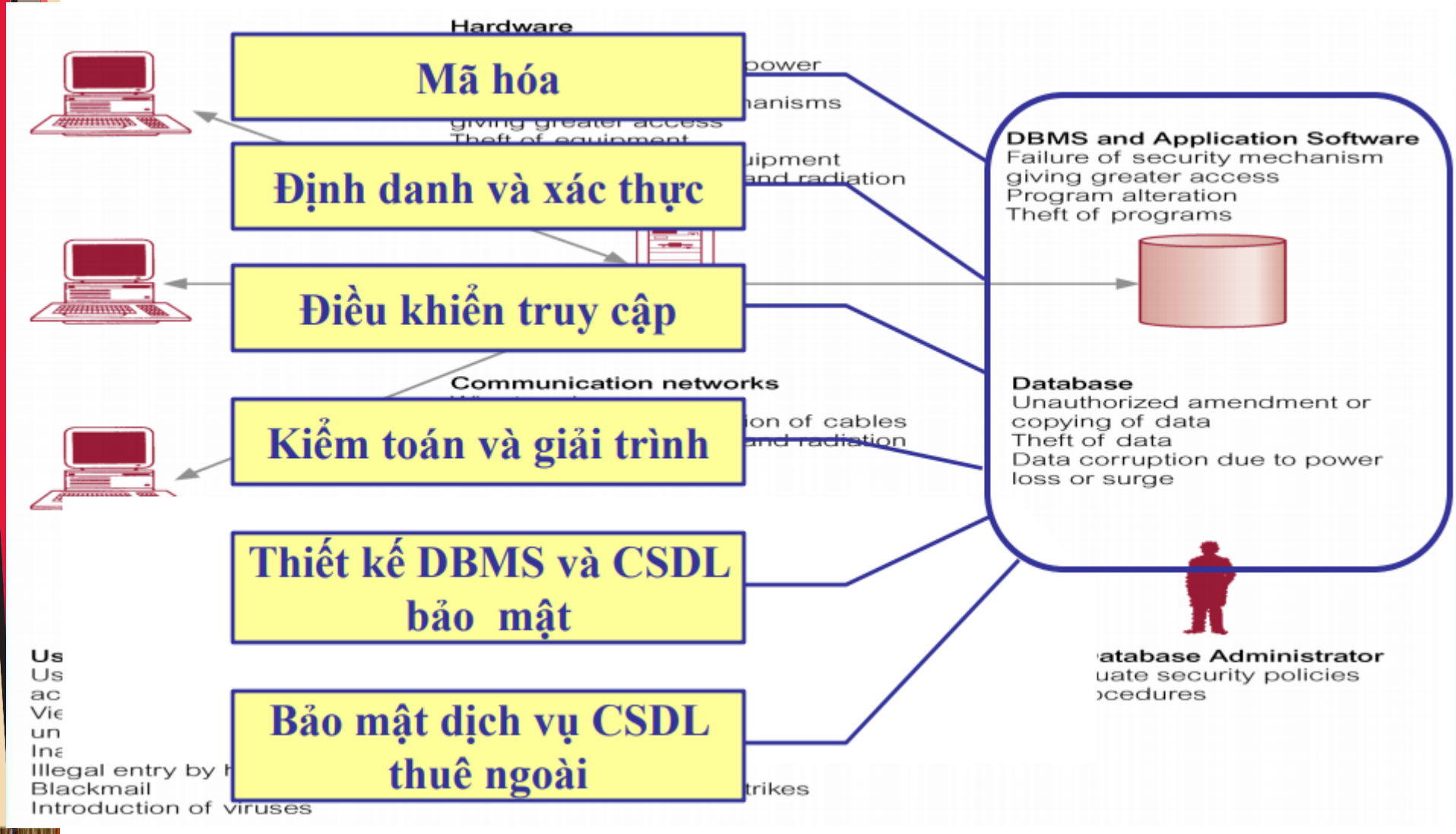
Các thành phần cần bảo vệ trong hệ thống thông tin



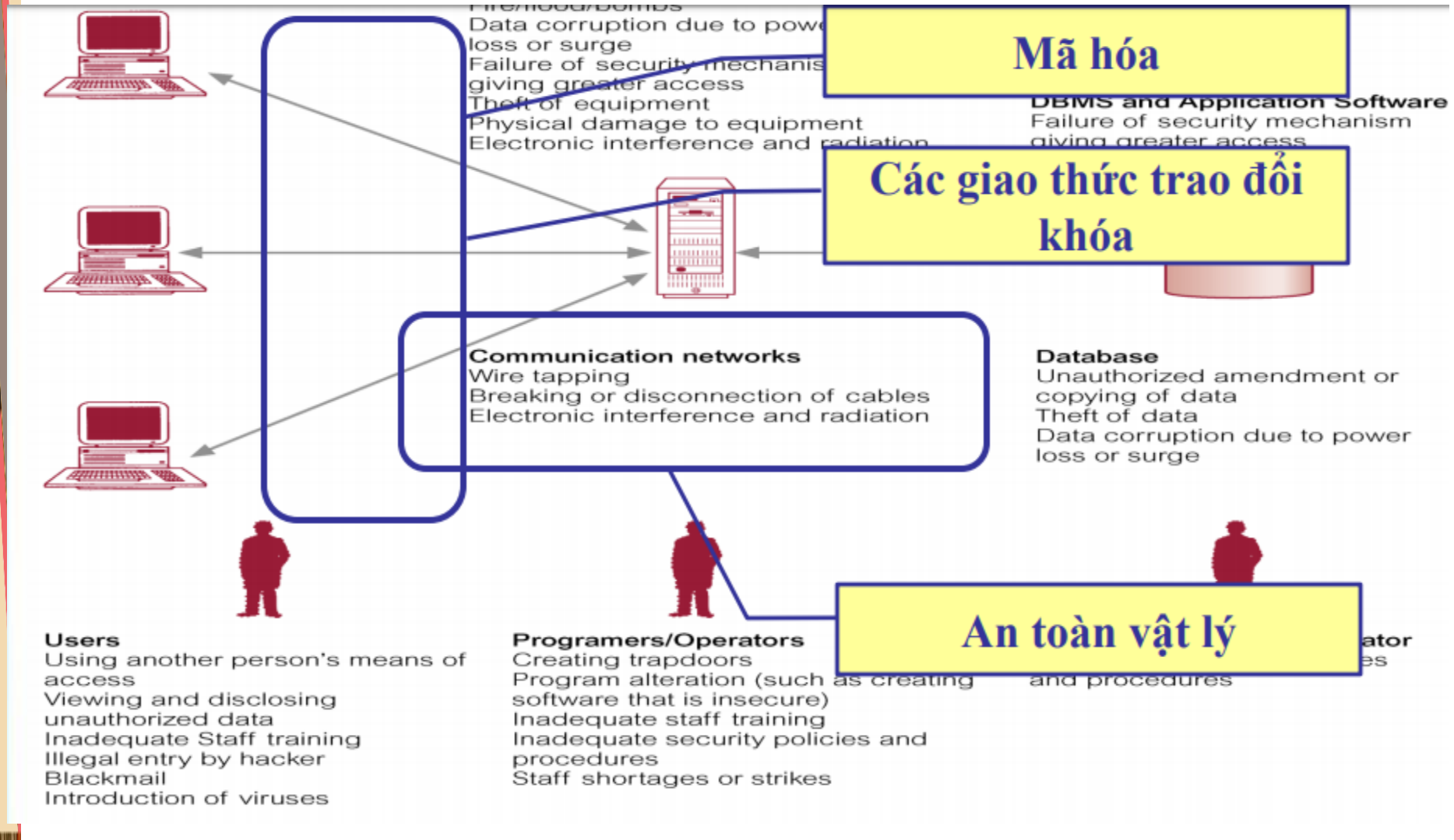
Các thành phần cần bảo vệ trong một HTTT

- Phần cứng
- Mạng
- Cơ sở dữ liệu (CSDL)
- Hệ quản trị CSDL (database management system - DMBS), các ứng dụng
- Người dùng
- Người lập trình hệ thống
- Người quản trị CSDL

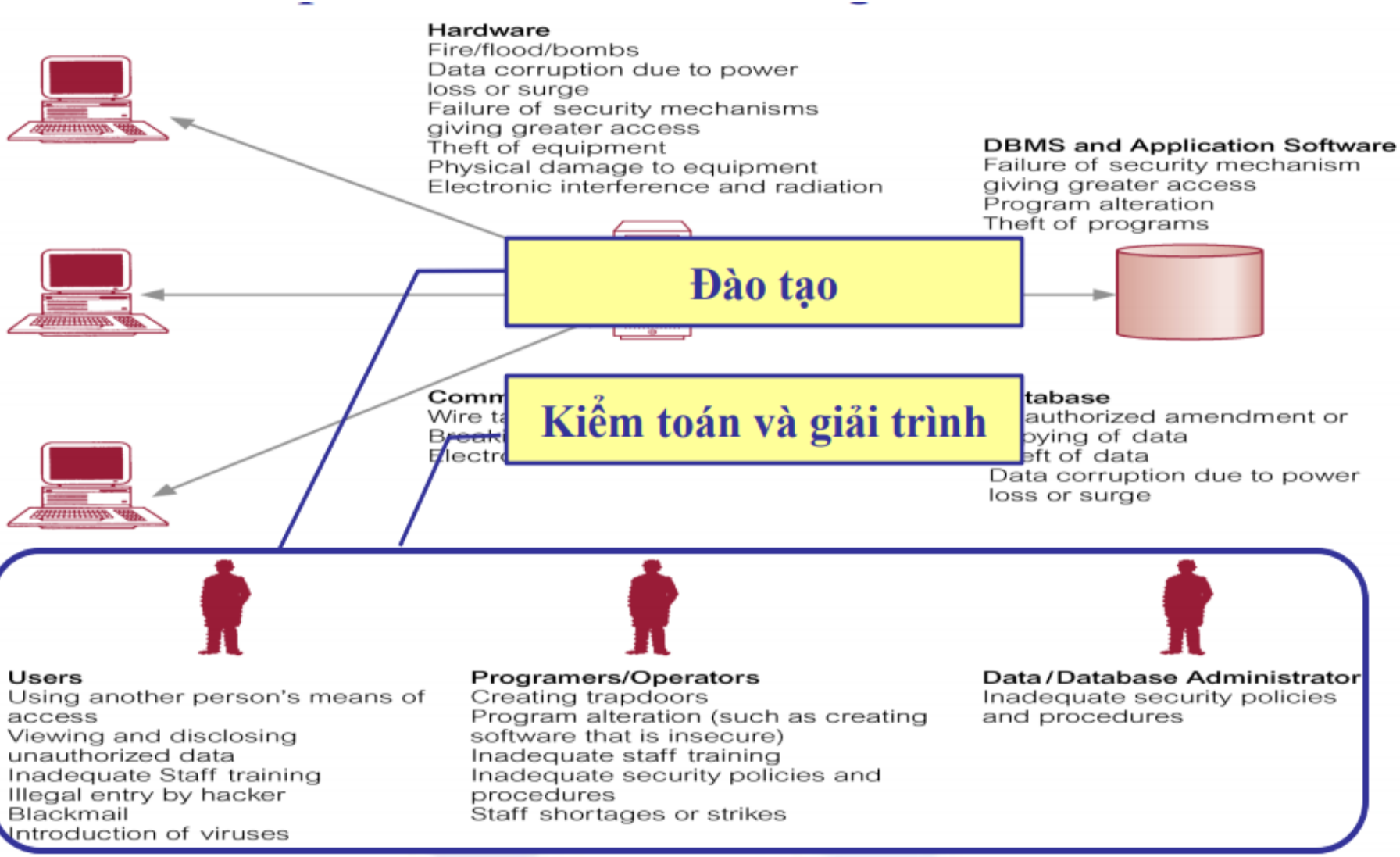
Các phương pháp bảo vệ HTTT



Các phương pháp bảo vệ HTTT



Các phương pháp bảo vệ HTTT



CÂU HỎI VÀ BÀI TẬP

1. Phân biệt dữ liệu (data) và thông tin (information), cho ví dụ từng loại
2. Hệ thống thông tin là gì? Hãy cho ví dụ một hệ thống thông tin mà bạn biết. Đưa ra dữ liệu/thông tin/chức năng nào cần đảm bảo an toàn, nêu lý do
3. Tam giác CIA là gì? Nêu mối tương quan giữa C, I, A
4. Trình bày tính xác thực và tính chống thoái thác? Cho ví dụ?
5. Trình bày và phân tích các giải pháp bảo đảm ATTT?
6. Trình bày tổng quan về thực trạng ATTT trên thế giới và tại Việt Nam?

CÂU HỎI VÀ BÀI TẬP

Bài tập 1:

- Liệt kê những thông tin cá nhân nào của bạn cần an toàn, nêu lý do tại sao (nếu mất an toàn thì hậu quả như thế nào)
- Hãy đưa ra những biện pháp an toàn thông tin cho từng thông tin cá nhân đã liệt kê ở trên

Bài tập 2:

- Đưa ra một doanh nghiệp mà bạn biết (nêu tên, lĩnh vực hoạt động)
- Nêu ra một HTTT của DN và mục tiêu của HTTT đó
- Liệt kê ra những thông tin/dữ liệu của doanh nghiệp đó cần an toàn, nêu lý do tại sao (nếu mất an toàn thì hậu quả như thế nào – phân tích hậu quả)

CÂU HỎI VÀ BÀI TẬP (tiếp)

- Công ty VCCloud là một trong nhiều công ty viễn thông, cung cấp các dịch vụ CDN cho các cá nhân và doanh nghiệp tại Việt Nam. Dịch vụ CDN là mạng lưới gồm nhiều máy chủ lưu trữ đặt tại nhiều vị trí địa lý khác nhau, cùng làm việc chung để phân phối nội dung, truyền tải hình ảnh, CSS, Javascript, Video clip, Real-time media streaming, File download đến người dùng cuối. Cơ chế hoạt động của CDN giúp cho khách hàng truy cập nhanh vào dữ liệu máy chủ web gần họ nhất thay vì phải truy cập vào dữ liệu máy chủ web tại trung tâm dữ liệu.
- Hãy nêu và giải thích ít nhất 4 tính cần thiết của an toàn HTTT đối với công ty/doanh nghiệp được mô tả ở trên

CÂU HỎI VÀ BÀI TẬP (tiếp)

- BẢO HIỂM MANULIFE Là thành viên của Manulife Financial, Manulife Việt Nam tự hào là doanh nghiệp bảo hiểm nhân thọ nước ngoài đầu tiên có mặt tại Việt Nam từ năm 1999 và sở hữu tòa nhà trụ sở riêng có với giá trị đầu tư hơn 10 triệu USD. Với bề dày kinh nghiệm và uy tín toàn cầu, Manulife đặt mục tiêu trở thành công ty bảo hiểm nhân thọ chuyên nghiệp nhất tại Việt Nam.
  Manulife Việt Nam hiện đang cung cấp một danh mục các sản phẩm đa dạng từ sản phẩm bảo hiểm truyền thống đến sản phẩm bảo hiểm sức khoẻ, giáo dục, liên kết đầu tư, hưu trí… cho hơn 700.000 khách hàng thông qua đội ngũ đại lý hùng hậu và chuyên nghiệp tại 55 văn phòng trên 40 tỉnh thành cả nước.
- Hãy nêu và giải thích ít nhất 4 tính cần thiết của an toàn HTTT đối với công ty/doanh nghiệp được mô tả ở trên

THANKS YOU