INDUSTRIAL UNIVERSITY OF HOCHIMINH CITY

Chương 1:
TỔNG QUAN VỀ AN TOÀN THÔNG TIN
(OVERVIEW OF INFORMATION SECURITY)

Nội dung

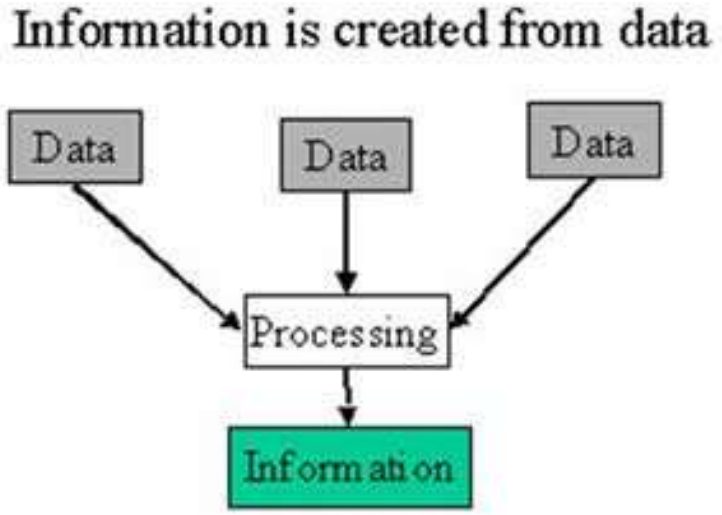
- Khái niệm cơ bản
- Mục tiêu của an toàn thông tin
- Tầm quan trọng An toàn thông tin đối với cá nhân/doanh nghiệp và xã hội
- Các phương pháp đảm bảo an toàn thông tin

Dữ liệu và 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 chưa xử lý được gọi là dữ liệu thô (Raw data),
  - Dữ liệu được trình bày dưới dạng: các con số, các từ, hình ảnh, âm thanh, đa phương tiện, dữ liệu động
- Hãy cho ví dụ một vài dữ liệu

Dữ liệu và 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 nghĩa đối với người được nhận nó.
- Cho ví dụ vài 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

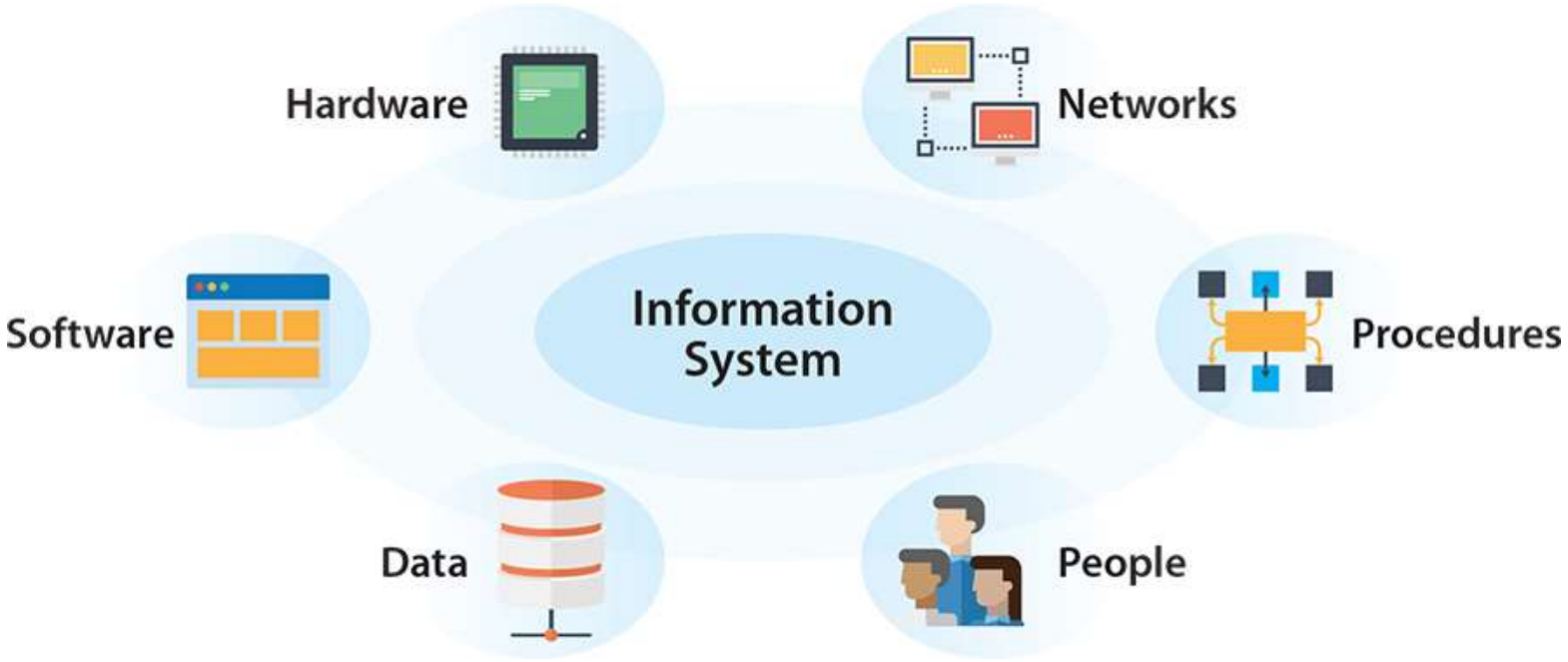
Section: 2

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

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

Hệ thống thông tin

- Hệ thống thông tin (Information systems)



An toàn thông tin

- **Information Security**
  - 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
  - An toàn thông tin mạng (information security), an toàn máy tính (computer security), đảm bảo thông tin (information assurance) được sử dụng hoán đổi cho nhau.

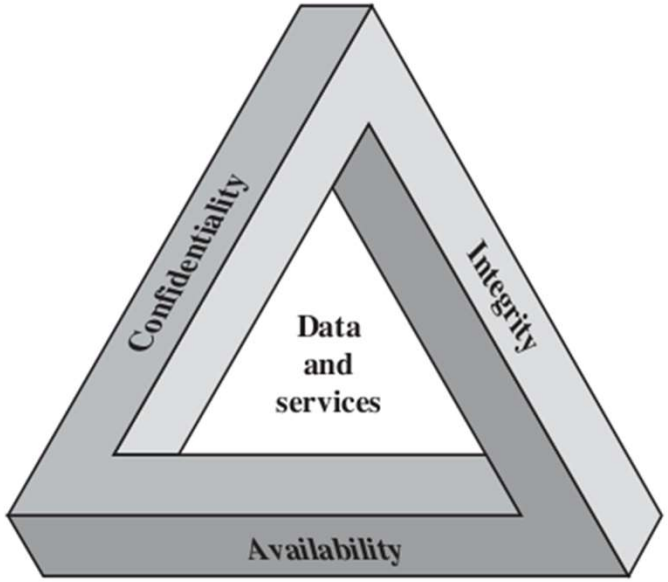
Tại sao cần an toàn thông tin?

- **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 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.

2. Mục tiêu của an toàn thông tin

- Ba khái niệm ATTT cần đảm bảo:
  - ***Tính bảo mật (Confidentiality),***
  - ***Tính toàn vẹn* (Integrity) và**
  - ***Tính sẵn dùng (Availability)***

  hình thành một ***Tam giác bảo mật CIA*** (CIA triad).
- Ba khái niệm thể hiện các mục tiêu cốt lõi an toàn cho cả thông tin và dịch vụ của hệ thống thông tin



2. Mục tiêu an toàn thông tin

- Tính bảo mật (Confidentiality)
  - Là nguyên tắc đảm bảo kiểm soát truy cập thông tin.
  - Thông tin chỉ được phép truy cập bởi những đối tượng (người, chương trình máy tính…) được cấp phép.
- Ví dụ: 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.

2. Mục tiêu an toàn thông tin

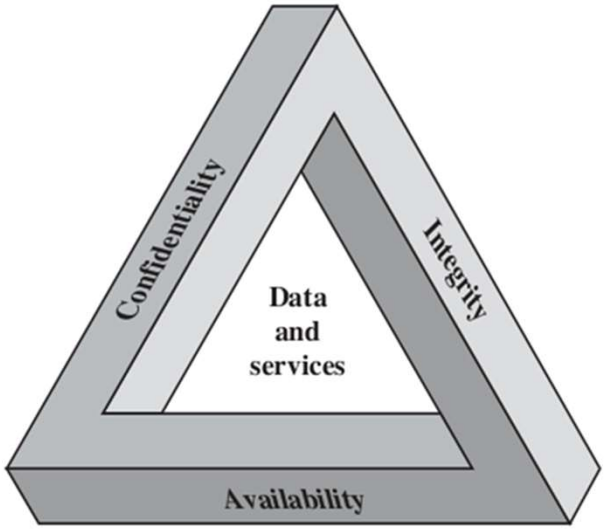
- Tính toàn vẹn (Integrity)
  - Là sự đảm bảo dữ liệu là đáng tin cậy và chính xác.
  - Thông tin **chỉ được phép xóa hoặc sửa bởi những đối tượng được phép và phải đảm bảo rằng thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi**.
- Ví dụ: Trong hệ thống ngân hàng, không cho phép khách hàng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

2. Mục tiêu an toàn thông tin

- Tính sẵn dùng (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 thông tin ngân hàng, cần đảm bảo rằng chủ tài khoản có thể truy vấn/giao dịch thông tin tài khoản 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%.

2. Mục tiêu an toàn thông tin

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



X$ = C + I + A

2. Mục tiêu 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 và 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.

2. Mục tiêu an toàn thông tin

- Bên cạnh bộ ba CIA, trong lĩnh vực an toàn còn khái niệm quan trọng cần có:
  - **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
  - **Tính chống thoái thác (Non-repudiation)**: Khả năng ngăn chặn việc từ chối một hành vi đã làm. Bên giao dịch không thể phủ nhận việc họ đã thực hiện giao dịch với các bên khác.
  - 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....

3. 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 chức
    - 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.

3. An toàn thông tin đối với một tổ chức

An toàn thông tin của của một tổ chức bị mất thì điều gì xảy ra?

4. Giải pháp để ATTT

4. Giải pháp để ATTT

4. Giải pháp để ATTT

Một số giải pháp

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