Chương 1:
Tổng quan về Bảo mật Hệ thống Thông tin

Khoa Khoa học và Kỹ thuật Máy tính
Đại học Bách Khoa Tp.HCM

Nội dung

1. Các khái niệm cơ bản
2. Các bước cơ bản trong bảo mật thông tin
3. Các thành phần trong hệ thống thông tin

Những khái niệm cơ bản

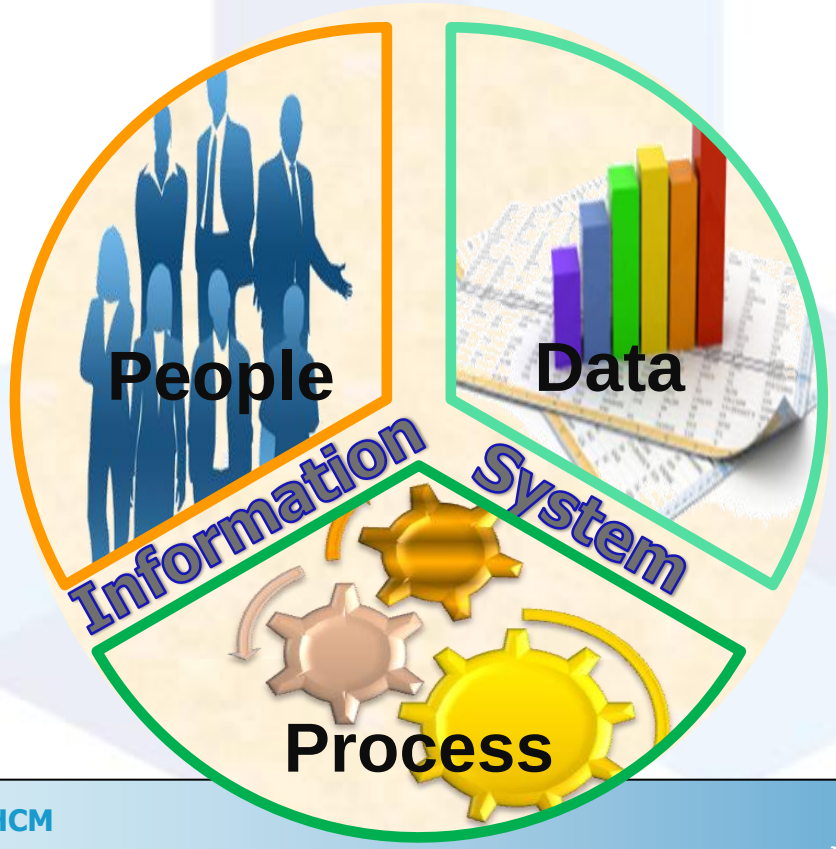
- Dữ liệu và thông tin
- Hệ thống thông tin
- Bảo mật thông tin
- Những yêu cầu bảo mật hệ thống thông tin
- Mục tiêu của bảo mật

Dữ liệu và thông tin

- ***Dữ liệu (Data)*** là *các giá trị của thông tin định lượng hoặc đính tính* của các sự vật, hiện tượng trong cuộc sống.Trong tin học, dữ liệu được dùng như một cách biểu diễn hình thức hoá của thông tin về các sự kiện, hiện tượng thích ứng với các yêu cầu truyền nhận, thể hiện và xử lí bằng máy tính.
- ***Thông tin (Information)*** là *dữ liệu đã được xử lý, phân tích, tổ chức* nhằm mục đích hiểu rõ hơn sự vật, sự việc, hiện tượng theo một góc độ nhất định.

Hệ thống thông tin

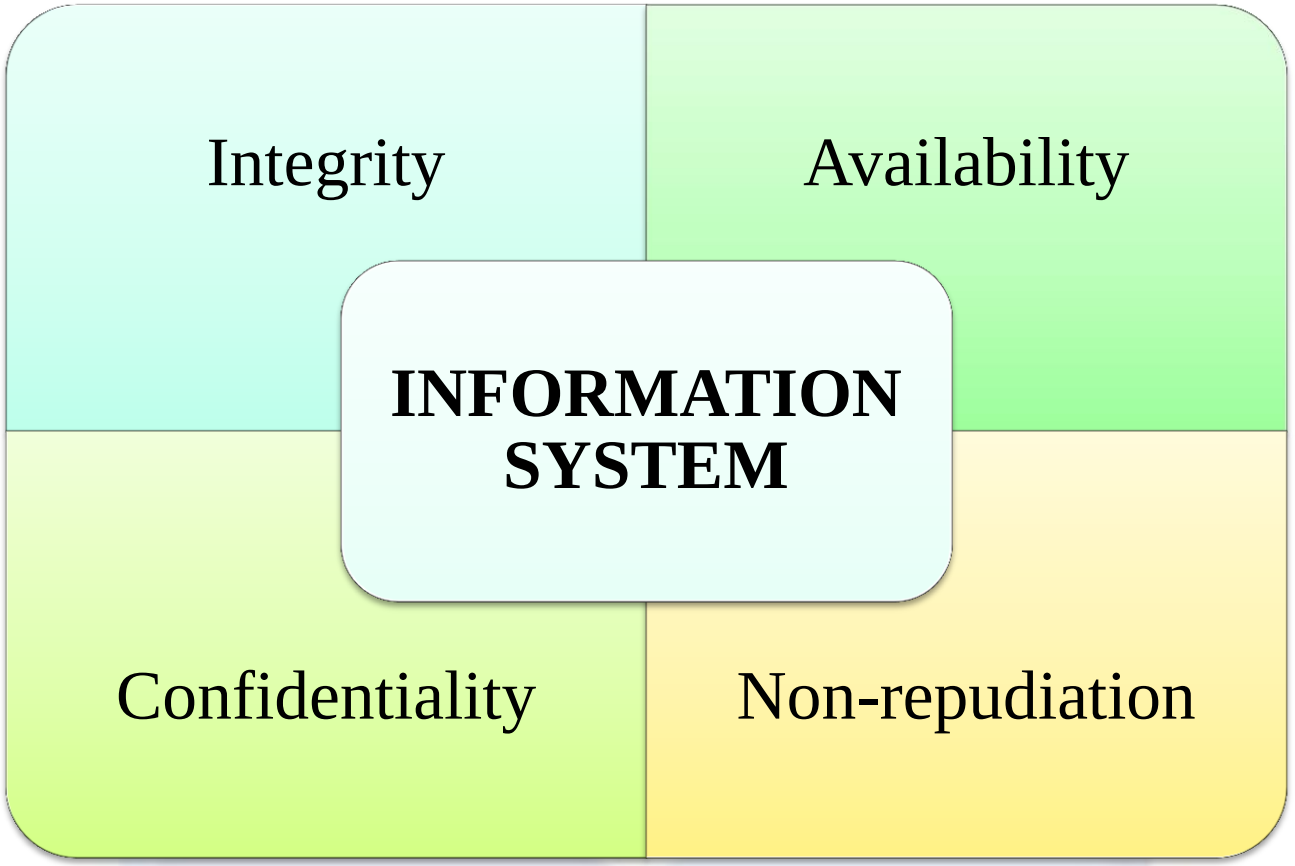
- ***Hệ thống thông tin (Information Systems)*** là một hệ thống gồm con người, dữ liệu và những hoạt động xử lý dữ liệu và thông tin trong một tổ chức.



Bảo mật hệ thống thông tin

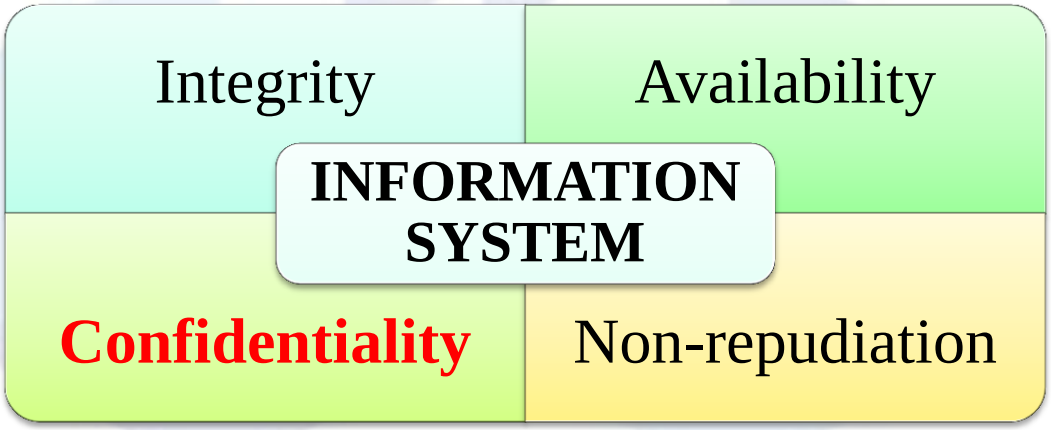
- ***Bảo mật hệ thống thông tin (Information Systems Security)*** là bảo vệ hệ thống thông tin chống lại việc truy cập, sử dụng, chỉnh sửa, phá hủy, làm lộ và làm gián đoạn thông tin và hoạt động của hệ thống một cách trái phép.

Những yêu cầu bảo mật hệ thống thông tin



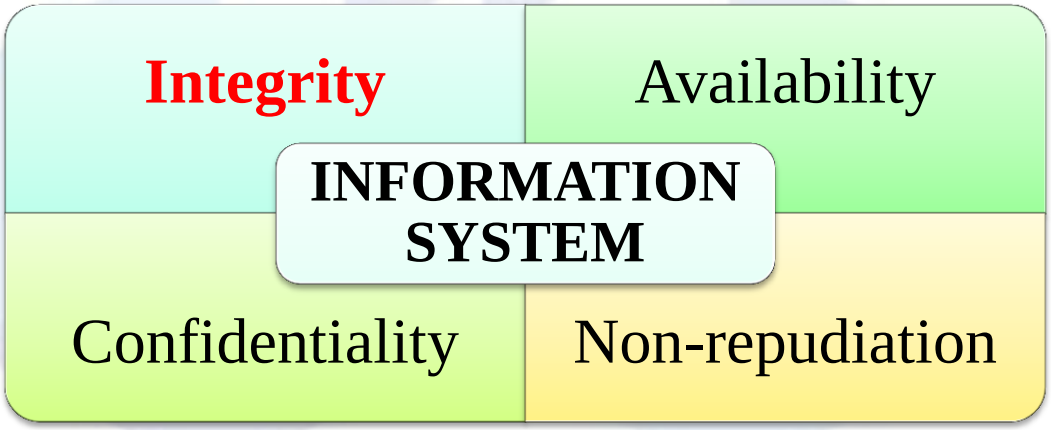
Những yêu cầu bảo mật hệ thống thông tin

- ***Tính bí mật (Confidentiality)***: bảo vệ dữ liệu không bị lộ ra ngoài một cách trái 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.



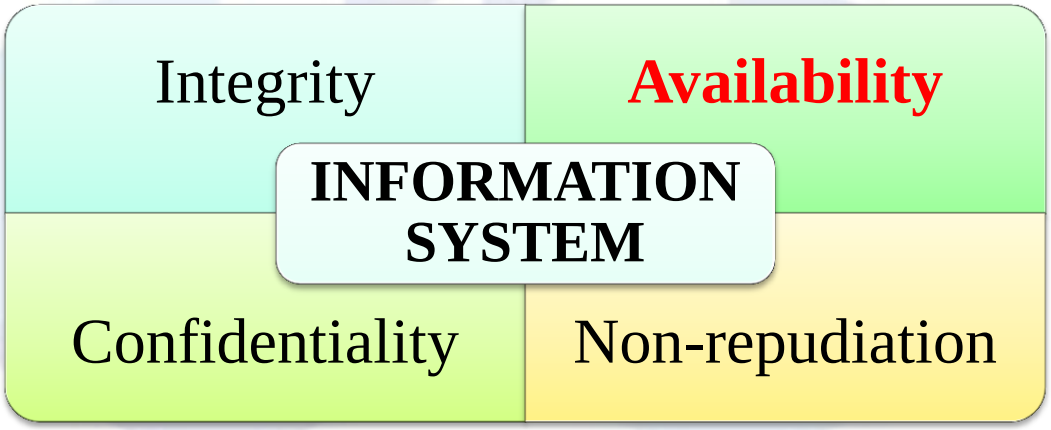
Những yêu cầu bảo mật hệ thống thông tin

- ***Tính toàn vẹn (Integrity)***: Chỉ những người dùng được ủy quyền mới được phép chỉnh sửa dữ liệu.
  - Ví dụ: Trong hệ thống ngân hàng, không cho phép khách hàng tự thay đổi thông tin số dư của tài khoản của mình.



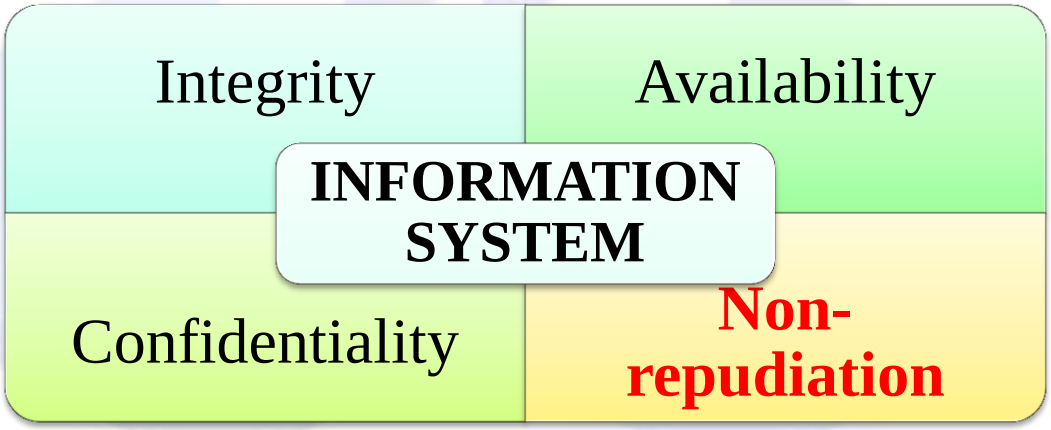
Những yêu cầu bảo mật hệ thống thông tin

- ***Tính sẵn sàng (Availability)***: Đảm bảo dữ liệu luôn sẵn sàng khi những người dùng hoặc ứng dụng được ủy quyền yêu cầu.
  - Ví dụ: Trong hệ thống ngân hàng, cần đảm bảo rằng khách hàng có thể truy vấn thông tin số dư tài khoản bất kỳ lúc nào theo như quy định.



Những yêu cầu bảo mật hệ thống 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 ngân hàng, có khả năng cung cấp bằng chứng để chứng minh một hành vi khách hàng đã làm, như rút tiền, chuyển tiền.



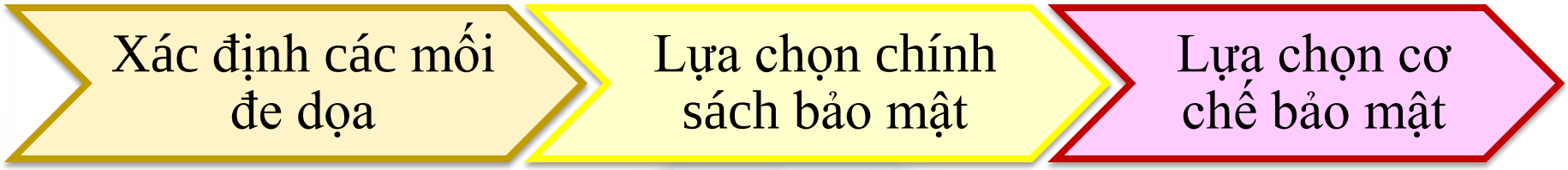
Mục tiêu của bảo mật

- ***Ngăn chặn***
  - Ngăn chặn kẻ tấn công vi phạm các chính sách bảo mật
- ***Phát hiện***
  - Phát hiện các vi phạm chính sách bảo mật
- ***Phục hồi***
  - Chặn các hành vi vi phạm đang diễn ra, đánh giá và sửa lỗi
  - Tiếp tục hoạt động bình thường ngay cả khi tấn công đã xảy ra

Nội dung

1. Các khái niệm cơ bản
2. Các bước cơ bản trong bảo mật thông tin
3. Các thành phần trong hệ thống thông tin

Các bước cơ bản trong bảo mật thông tin



- Xác định các mối đe dọa (threat)
  - Cái gì có thể làm hại đến hệ thống?
- Lựa chọn chính sách bảo mật (security policy)
  - Điều gì cần mong đợi ở hệ thống bảo mật?
- Lựa chọn cơ chế bảo mật (security mechanism)
  - Cách nào để hệ thống bảo mật có thể đạt được những mục tiêu bảo mật đề ra?

Xác định các mối nguy hiểm

Xác định các mối đe dọa | Lựa chọn chính sách bảo mật | Lựa chọn cơ chế bảo mật

- Các mối đe dọa bảo mật (security threat) là những sự kiện có ảnh hưởng đến an toàn của hệ thống thông tin.
- Các mối đe dọa được chia làm 4 loại:
  - Xem thông tin một cách bất hợp pháp
  - Chỉnh sửa thông tin một cách bất hợp pháp
  - Từ chối dịch vụ
  - Từ chối hành vi

Các mối đe dọa thường gặp

- Lỗi và thiếu sót của người dùng (Errors and Omissions)
- Gian lận và đánh cắp thông tin (Fraud and Theft)
- Kẻ tấn công nguy hiểm (Malicious Hackers)
- Mã nguy hiểm (Malicious Code)
- Tấn công từ chối dịch vụ (Denial-of-Service Attacks)
- Social Engineering

Lỗi và thiếu sót của người dùng

- Mối đe dọa của hệ thống thông tin xuất phát từ những lỗi bảo mật, lỗi thao tác của những người dùng trong hệ thống.
- Là mối đe dọa hàng đầu đối với một hệ thống thông tin
- Giải pháp:
  - Huấn luyện người dùng thực hiện đúng các thao tác, hạn chế sai sót
  - Nguyên tắc: quyền tối thiểu (least privilege)
  - Thường xuyên back-up hệ thống

Gian lận và đánh cắp thông tin

- Mối đe dọa này do những kẻ tấn công từ bên trong hệ thống (inner attackers), gồm những người dùng giả mạo hoặc những người dùng có ý đồ xấu.
- Những người tấn công từ bên trong luôn rất nguy hiểm.
- Giải pháp:
  - Định ra những chính sách bảo mật tốt: có chứng cứ xác định được kẻ tấn công từ bên trong

Kẻ tấn công nguy hiểm

- Kẻ tấn công nguy hiểm xâm nhập vào hệ thống để tìm kiếm thông tin, phá hủy dữ liệu, phá hủy hệ thống.
- 5 bước để tấn công vào một hệ thống:
  - Thăm dò (Reconnaisance)
  - Quét lỗ hổng để tấn công (Scanning)
  - Cố gắng lấy quyền truy cập (Gaining access)
  - Duy trì kết nối (Maintaining access)
  - Xóa dấu vết (Cover his track)

Mã nguy hiểm

- Mã nguy hiểm là một đoạn mã không mong muốn được nhúng trong một chương trình nhằm thực hiện các truy cập trái phép vào hệ thống máy tính để thu thập các thông tin nhạy cảm, làm gián đoạn hoạt động hoặc gây hại cho hệ thống máy tính.
- Bao gồm: virus, worm, trojan horses, spyware, adware, backdoor, …

Tấn công từ chối dịch vụ

- Là kiểu tấn công ngăn không cho những người dùng khác truy cập vào hệ thống
- Làm cho hệ thống bị quá tải và không thể hoạt động
- DoS: tấn công "one-to-one"
- DDoS(distributed denial of service)
  - Sử dụng các Zombie host
  - Tấn công "many-to-one"

Social Engineering

- Social engineering sử dụng sự ảnh hưởng và sự thuyết phục để đánh lừa người dùng nhằm khai thác các thông tin có lợi cho cuộc tấn công hoặc thuyết phục nạn nhân thực hiện một hành động nào đó
- Kẻ tấn công có thể lợi dụng các đặc điểm sau của con người để tấn công:
  - Mong muốn trở nên hữu dụng
  - Tin người
  - Nỗi sợ gặp rắc rối
  - Đơn giản đến mức cẩu thả

Có 2 loại Social Engineering

- Social engineering dựa trên con người liên quan đến sự tương tác giữa con người với con người để thu được thông tin mong muốn
- Social engineering dựa trên máy tính: liên quan đến việc sử dụng các phần mềm để cố gắng thu thập thông tin cần thiết

Social engineering dựa trên con người

- Nhân viên gián điệp/giả mạo
- Giả làm người cần được giúp đỡ
- Giả làm người quan trọng
- Giả làm người được ủy quyền
- Giả làm nhân viên hỗ trợ kỹ thuật

Social engineering dựa trên máy tính

- Phising: lừa đảo qua thư điện tử
- Vishing: lừa đảo qua điện thoại
- Pop-up Windows
- File đính kèm trong email
- Các website giả mạo
- Các phần mềm giả mạo

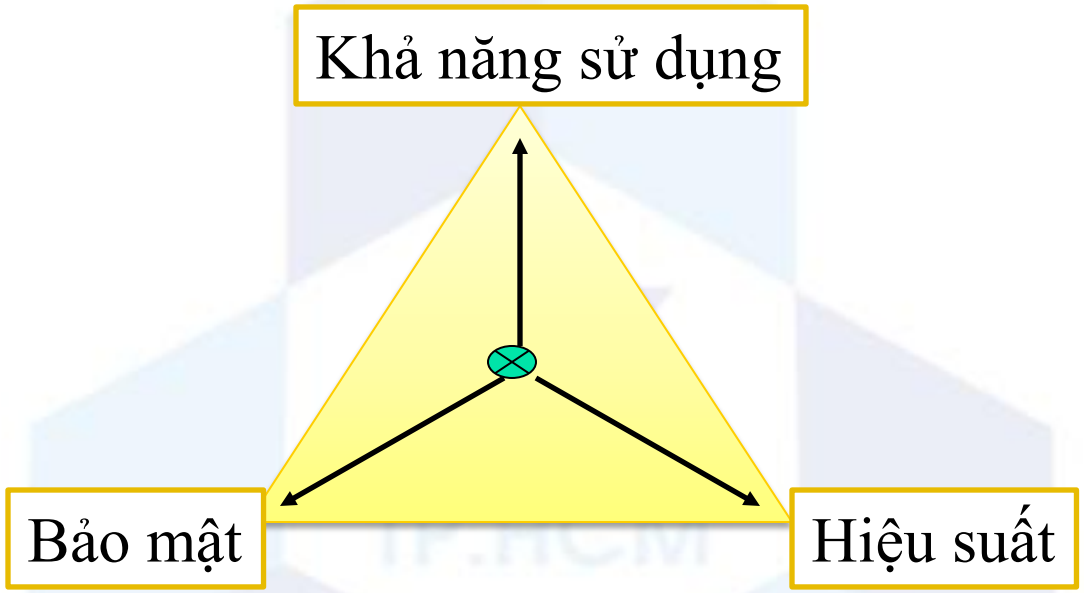
Lựa chọn chính sách bảo mật

Xác định các mối đe dọa | **Lựa chọn chính sách bảo mật** | Lựa chọn cơ chế bảo mật

- Việc bảo mật hệ thống cần có một chính sách bảo mật rõ ràng.
- Cần có những chính sách bảo mật riêng cho những yêu cầu bảo mật khác nhau
- Xây dựng và lựa chọn các chính sách bảo mật cho hệ thống phải dựa theo các chính sách bảo mật do các tổ chức uy tín về bảo mật định ra (compliance)
  - NIST, SP800, ISO17799, HIPAA

Lựa chọn chính sách bảo mật

- Chính sách bảo mật phải cân bằng giữa 3 yếu tố



Lựa chọn cơ chế bảo mật

- Xác định cơ chế bảo mật phù hợp để hiện thực các chính sách bảo mật và đạt được các mục tiêu bảo mật đề ra
- Có 4 cơ chế bảo mật:
  - Điều khiển truy cập (Access control)
  - Điều khiển suy luận (Inference control)
  - Điều khiển dòng thông tin (Flow control)
  - Mã hóa (Encryption)

Điều khiển truy cập

- ***Điều khiển truy cập (Access control)***: là cơ chế điều khiển, quản lý các truy cập vào hệ thống cơ sở dữ liệu.
- Các bước trong điều khiển truy cập

Định danh (Identification):
Người dùng cung cấp danh định (identity)

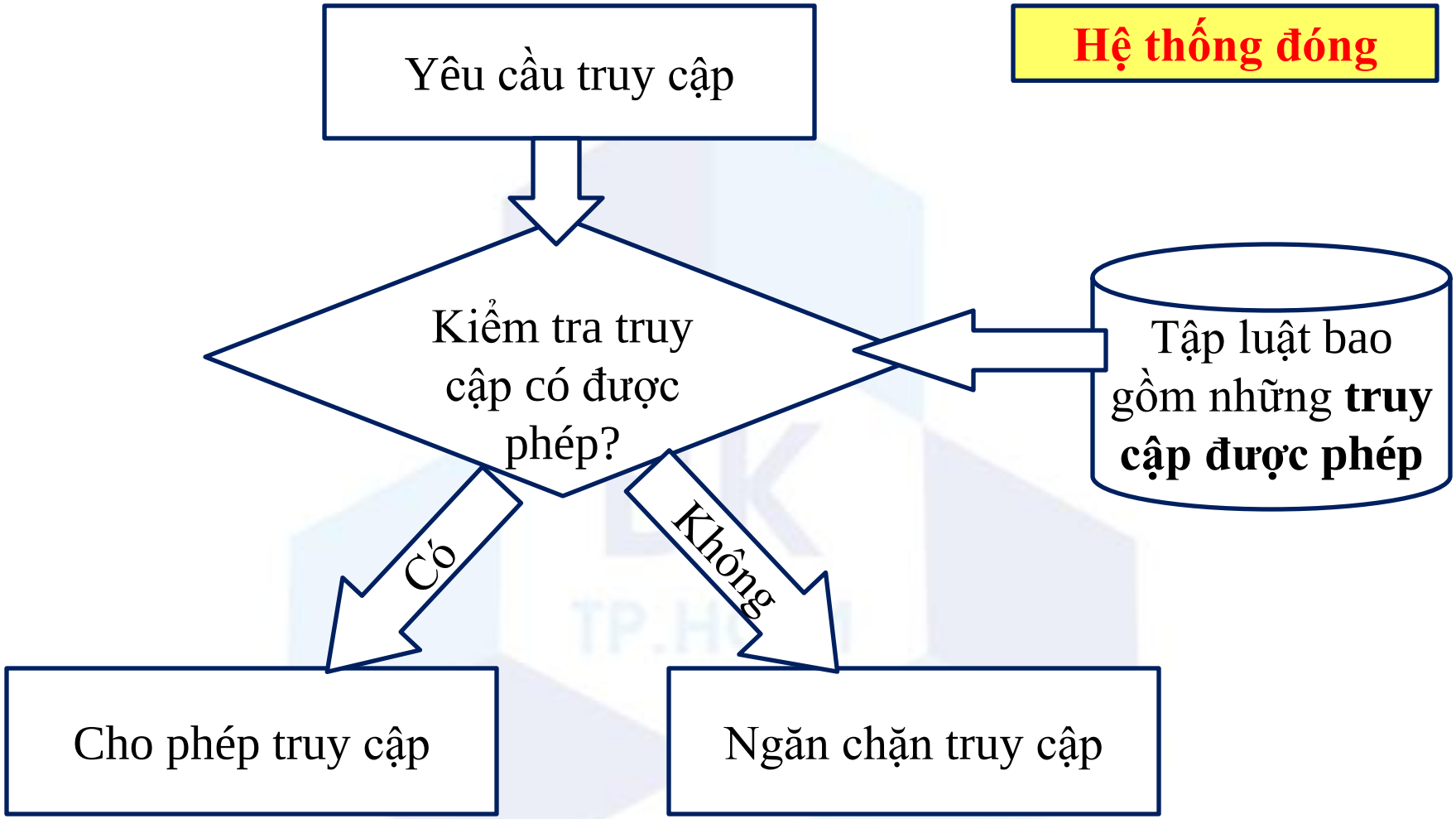
Xác thực (Authentication):
Người dùng chứng minh danh định đó là đúng

Ủy quyền (Authorization):
Xác định quyền mà người dùng có

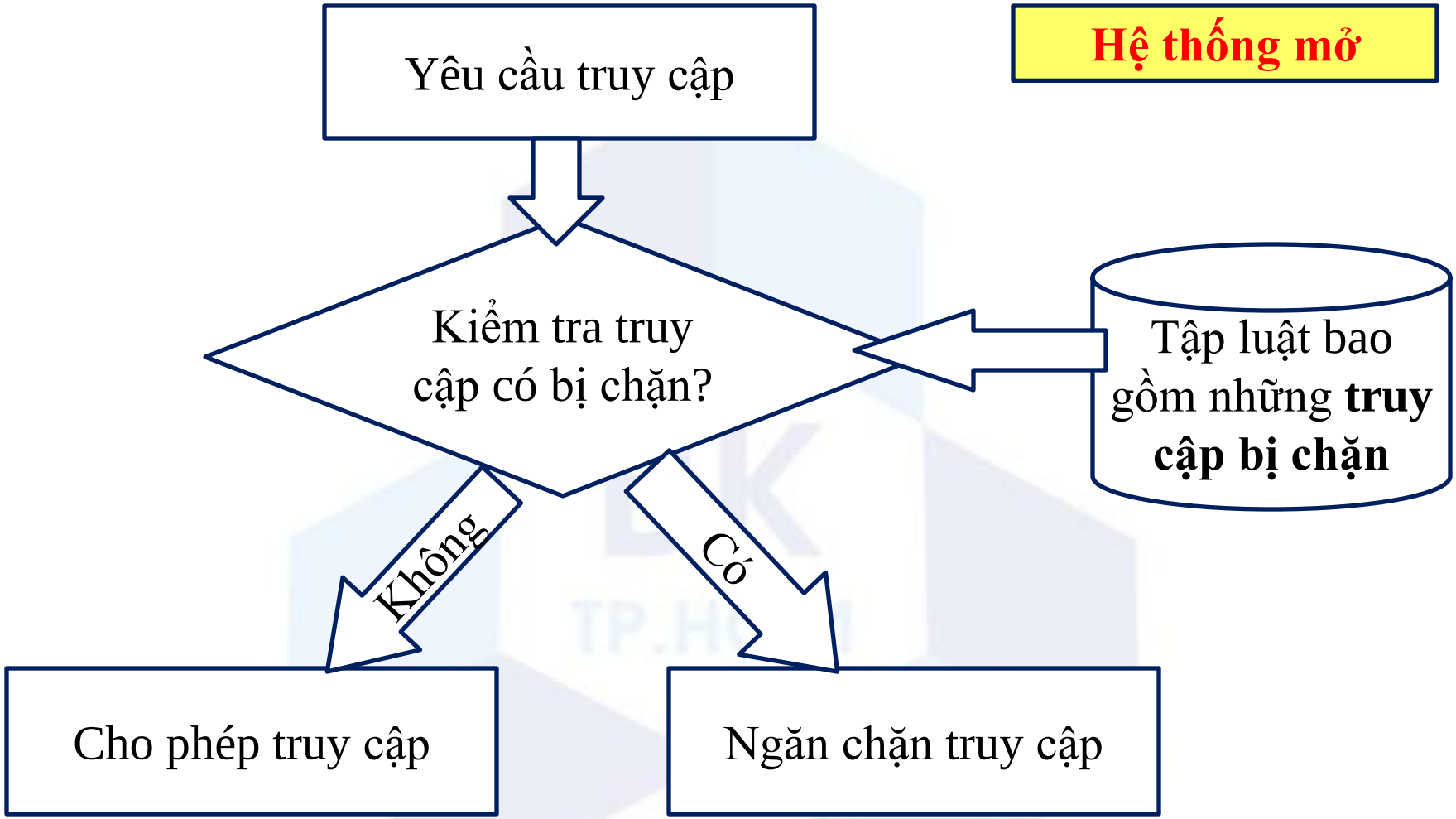
Điều khiển truy cập

- Có 2 loại hệ thống điều khiển truy cập
  - Hệ thống đóng (closed system)
  - Hệ thống mở (Open system)

Điều khiển truy cập – Hệ thống đóng



Điều khiển truy cập – Hệ thống mở



Điều khiển truy cập

- ***Cơ chế để xây dựng các tập luật điều khiển truy cập***: cách thức để xét một truy cập là cho phép hoặc bị từ chối
  - Điều khiển truy cập tùy quyền (Discretionary Access Control)
  - Điều khiển truy cập bắt buộc (Mandatory Access Control)

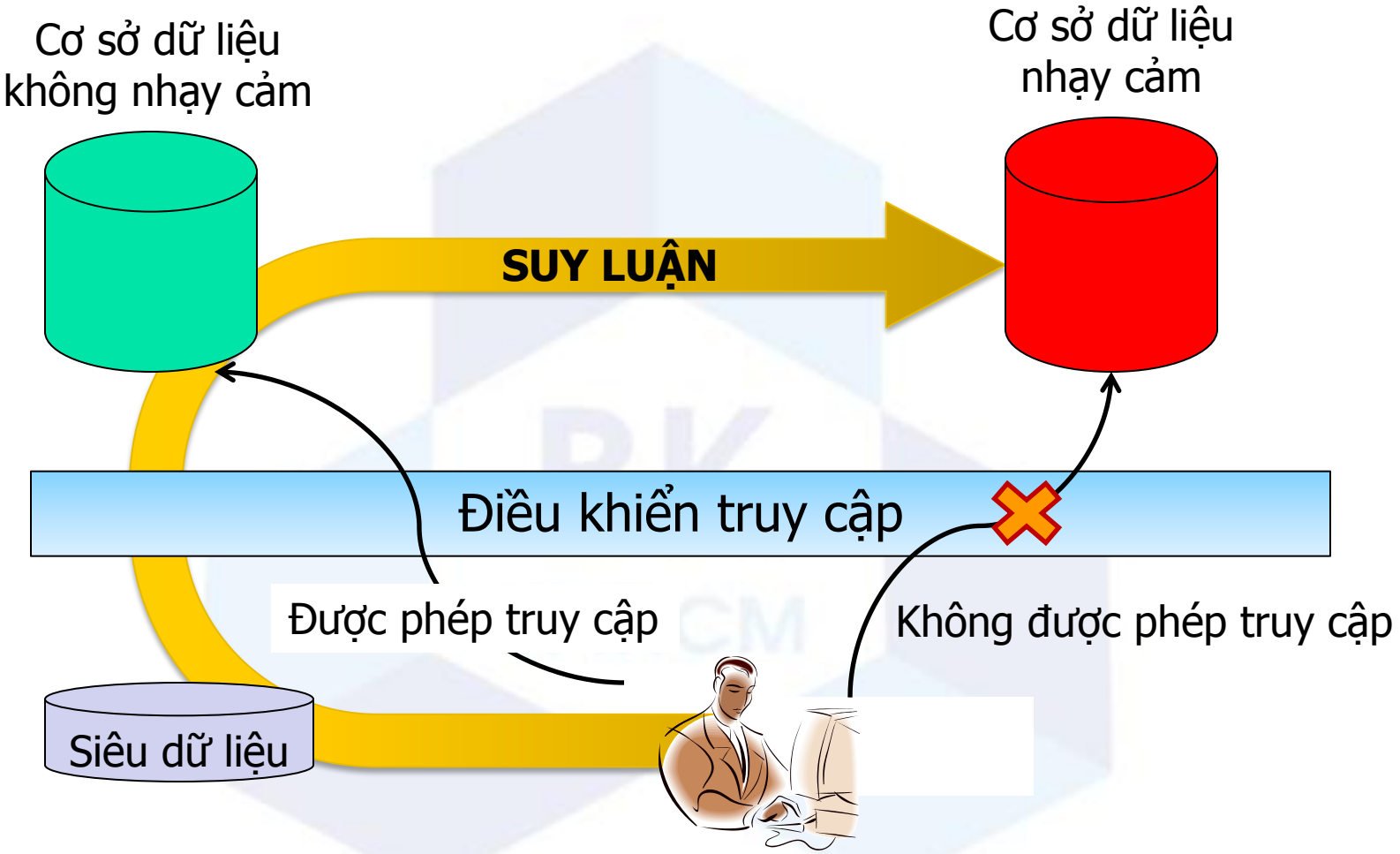
Điều khiển suy luận

- ***Điều khiển suy luận (Inference control)***: là việc quản lý, điền khiển các truy cập vào những cơ sở dữ liệu thống kê (statistical database) bởi vì từ những dữ liệu thống kê có thể suy luận ra được những thông tin nhạy cảm.
  - Tập dữ liệu X: user A có thể đọc
  - Tập dữ liệu Y: user A không được phép đọc

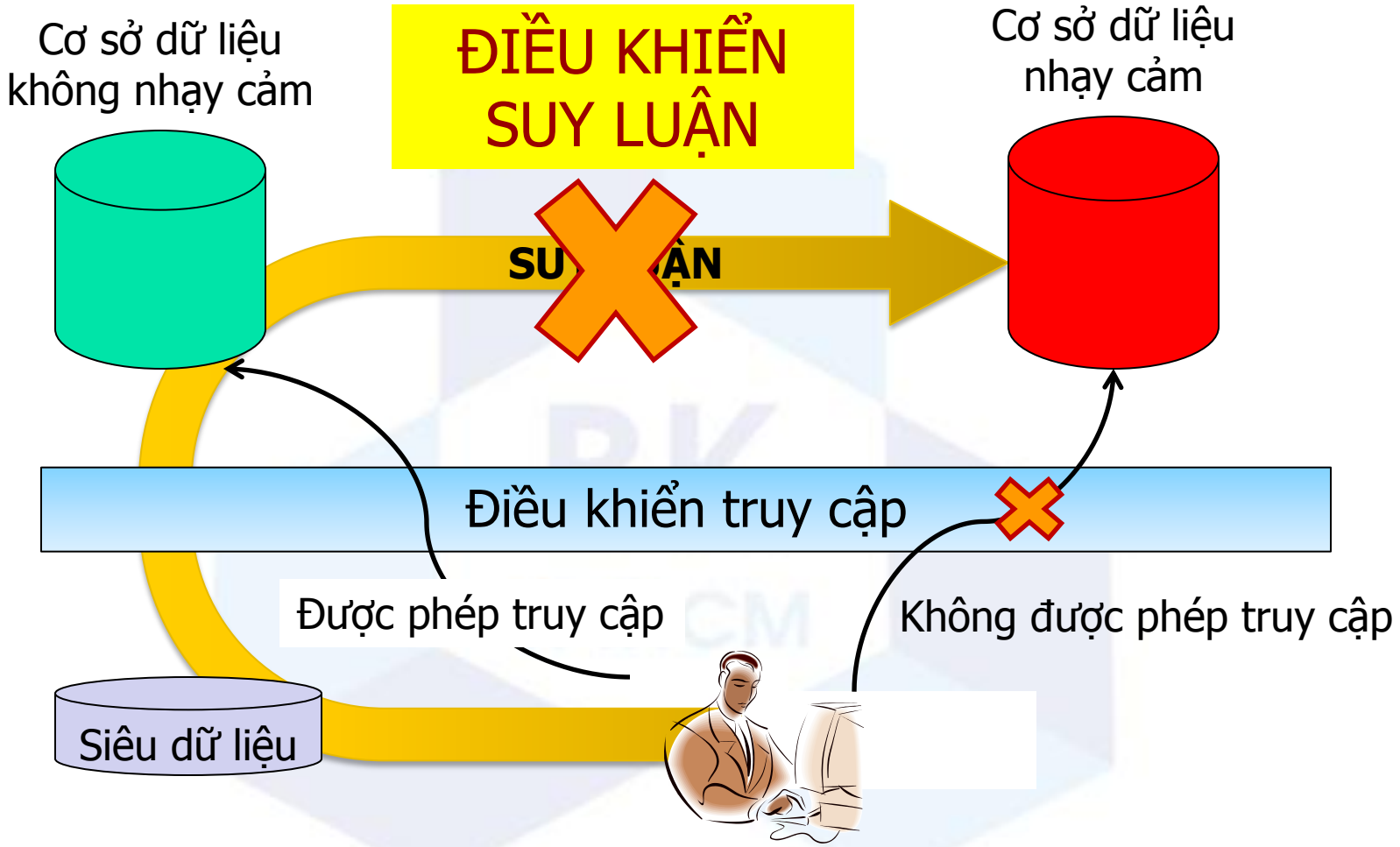
    … nhưng: Y = f(X)

  → Nếu user A biết được hàm f thì có thể tìm được tập Y (mà user A không được phép xem) từ tập X

Tấn công suy luận (Inference attack)



Điều khiển suy luận



Điều khiển dòng thông tin

- ***Dòng thông tin (Information flow)*** giữa đối tượng (object) X và đối tượng Y xảy ra khi có một chương trình đọc dữ liệu từ X và ghi vào Y.
- ***Điều khiển dòng thông tin (Flow control)*** nhằm ngăn chặn dòng thông tin đi từ đối tượng dữ liệu được bảo vệ sang đối tượng dữ liệu ít được bảo vệ hơn.

Điều khiển dòng thông tin

- ***Kênh biến đổi (Covert Channels)*** là những kênh truyền mà qua đó dòng thông tin có thể được truyền ngầm ra bên ngoài một cách bất hợp pháp. Có 2 loại convert channel:
  - Kênh lưu trữ (Storage channel): thông tin được truyền qua những đối tượng lưu trữ trung gian
  - Kênh thời gian (Timing channel): một phần thông tin có thể bị lộ ra ngoài thông qua thời gian tính toán các dữ liệu liên quan đến thông tin đó.

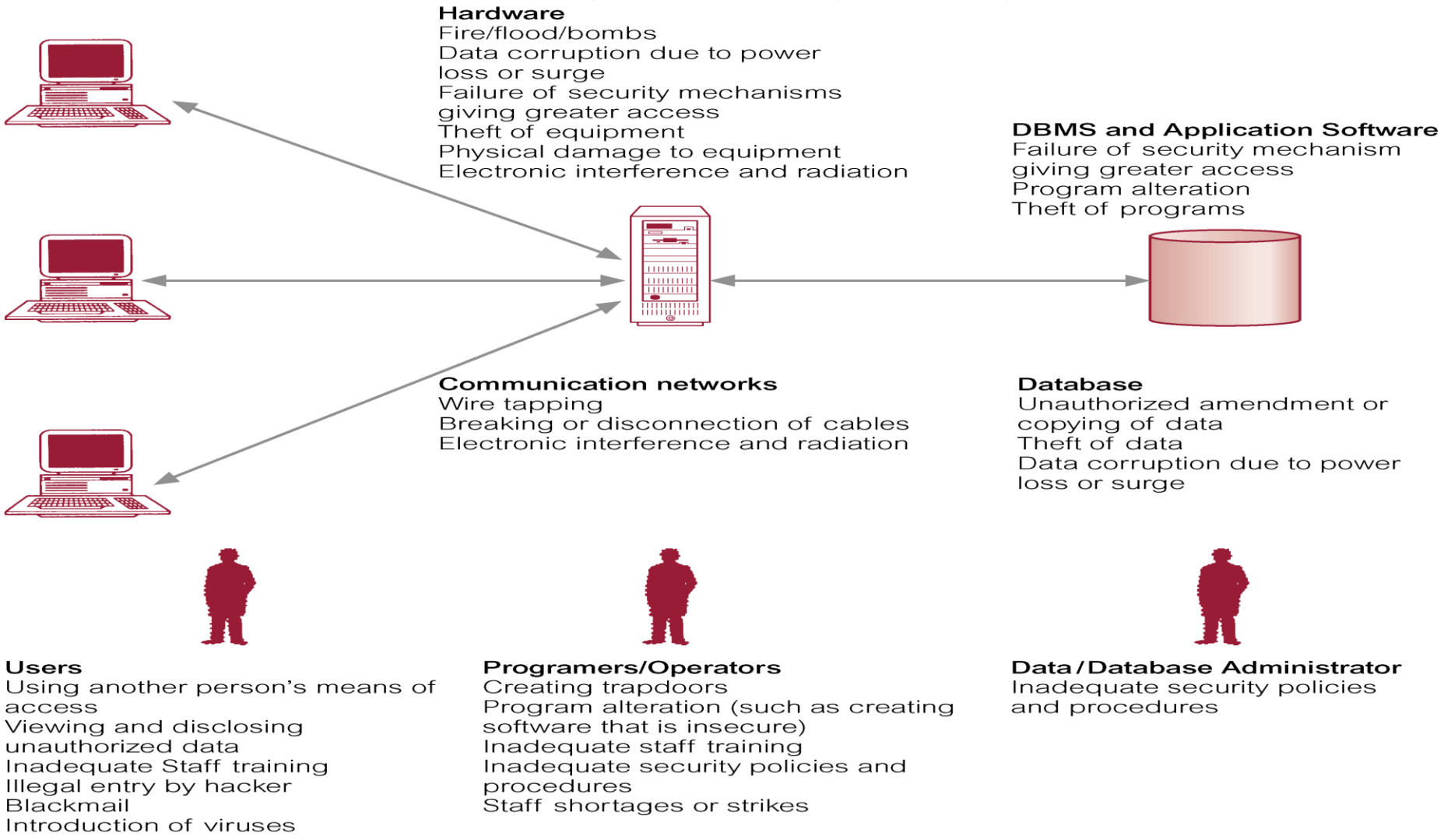
Mã hóa

- ***Mã hóa (Encryption)*** là những giải thuật tính toán nhằm chuyển đổi những văn bản gốc (plaintext), dạng văn bản có thể đọc được, sang dạng văn bản mã hóa (cyphertext), dạng văn bản không thể đọc được.
- Chỉ người dùng có được khóa đúng mới có thể giải mã được văn bản mã hóa về dạng văn bản rõ ban đầu.
- Mã hóa dữ liệu được sử dụng để bảo vệ những dữ liệu nhạy cảm.

Nội dung

1. Các khái niệm cơ bản
2. Các bước cơ bản trong bảo mật thông tin
3. Các thành phần trong hệ thống thông tin

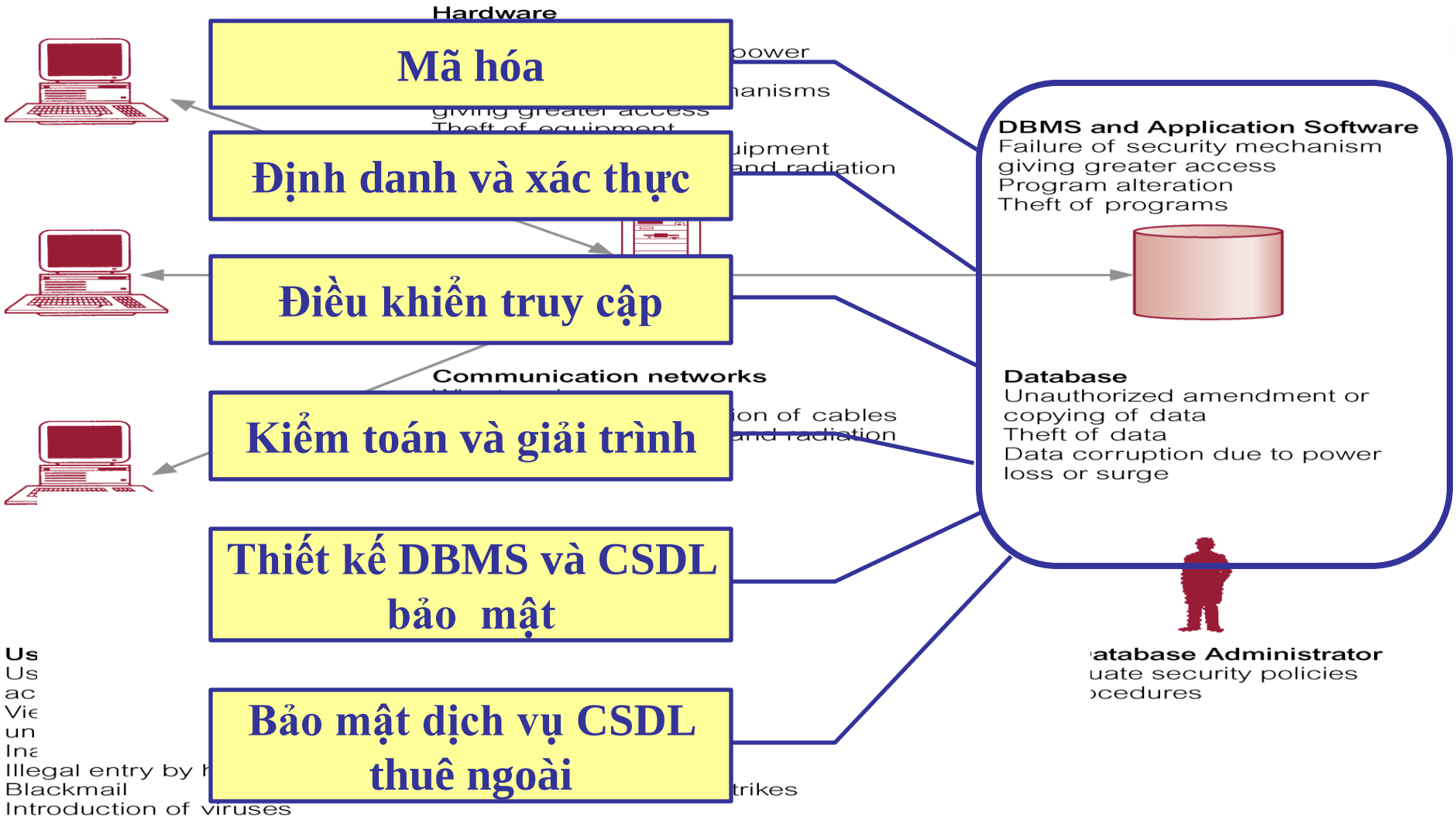
Các thành phần trong hệ thống thông tin



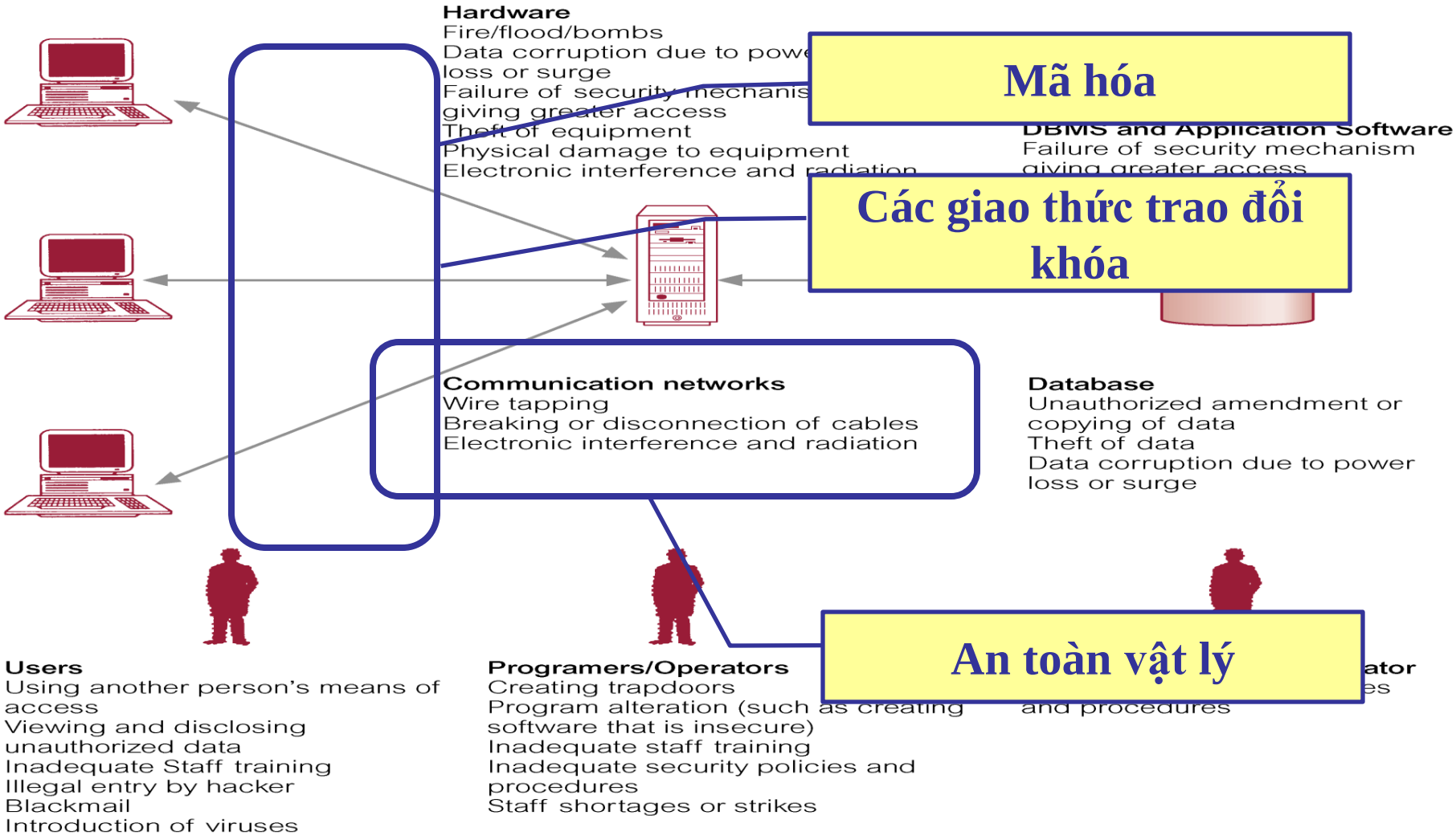
Các thành phần cần bảo vệ trong một HTTT

- 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

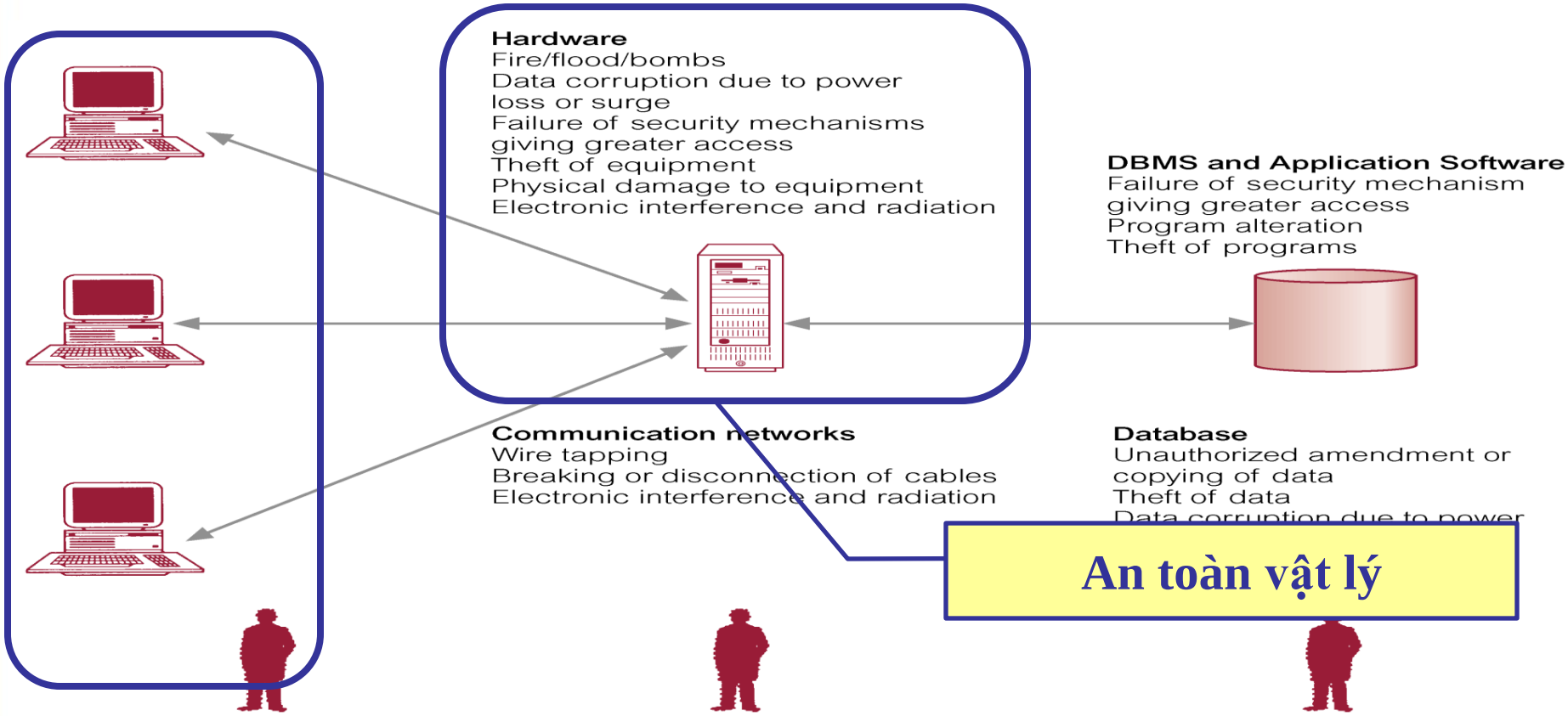
Các thành phần cần bảo vệ trong một HTTT



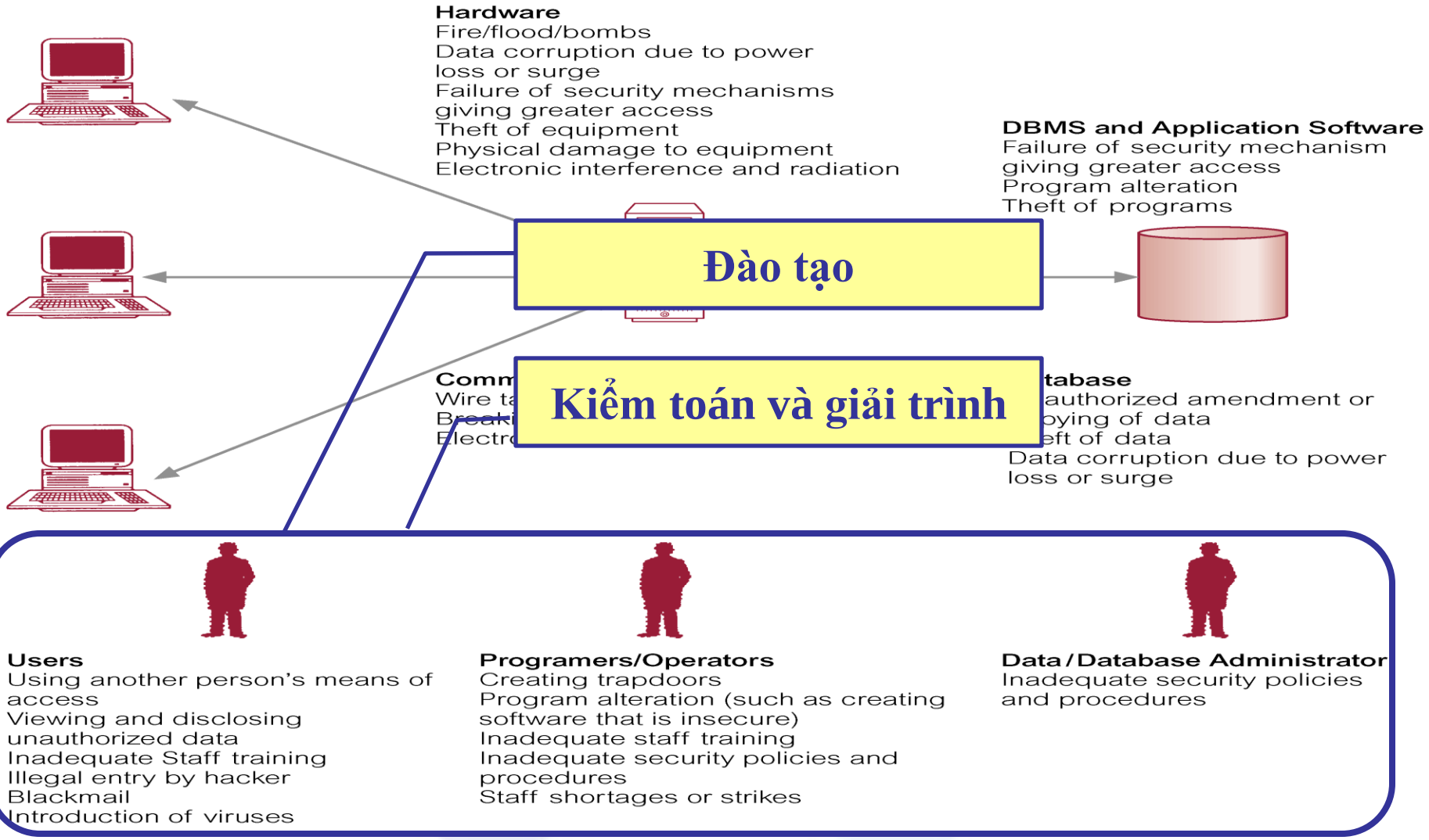
Các thành phần cần bảo vệ trong một HTTT



Các thành phần cần bảo vệ trong một HTTT



Các thành phần cần bảo vệ trong một HTTT




Question ?