HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI GIẢNG MÔN HỌC
AN TOÀN BẢO MẬT HỆ THỐNG THÔNG TIN

CHƯƠNG 1 – TỔNG QUAN VỀ AN TOÀN BẢO MẬT HỆ THỐNG THÔNG TIN

Giảng viên: TS. Hoàng Xuân Dậu

Điện thoại/E-mail: dauhx@ptit.edu.vn

Bộ môn: An toàn thông tin - Khoa CNTT1

TÀI LIỆU THAM KHẢO

1. Hoàng Xuân Dậu, Bài giảng An toàn và bảo mật hệ thống thông tin, Học viện Công nghệ BC-VT, 2017.
2. David Kim, Michael G. Solomon, *Fundamentals of Information Systems Security*, Jones & Bartlettlearning, 2012.
3. Michael E. Whitman, Herbert J. Mattord, *Principles of information security*, 4th edition, Course Technology, Cengage Learning, 2012.
4. Matt Bishop, *Introduction to Computer Security*, Prentice Hall, 2004.
5. William Stallings, *Cryptography and Network Security*, Prentice Hall, 2010.
6. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, October 1996.

ĐÁNH GIÁ MÔN HỌC

- Các điểm thành phần:
  - Chuyên cần: 10%
  - Kiểm tra: 10%
  - Bài tập+Tiểu luận: 20%
  - Thi cuối kỳ: 60%

NỘI DUNG MÔN HỌC

1. Tổng quan về an toàn bảo mật hệ thống thông tin
2. Các dạng tấn công và phần mềm độc hại
3. Đảm bảo an toàn thông tin dựa trên mã hóa
4. Các kỹ thuật, công nghệ và công cụ đảm bảo an toàn thông tin
5. Quản lý, chính sách và pháp luật an toàn thông tin.

NỘI DUNG CHƯƠNG 1

1. Giới thiệu về ATTT và an toàn hệ thống thông tin
2. Các yêu cầu an toàn hệ thống thông tin
3. Bảy vùng trong cơ sở hạ tầng CNTT và các mối đe dọa ATTT
4. Mô hình tổng quát đảm bảo an toàn hệ thống thông tin

1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

Tại sao cần phải đảm bảo an toàn cho thông tin và hệ thống thông tin?

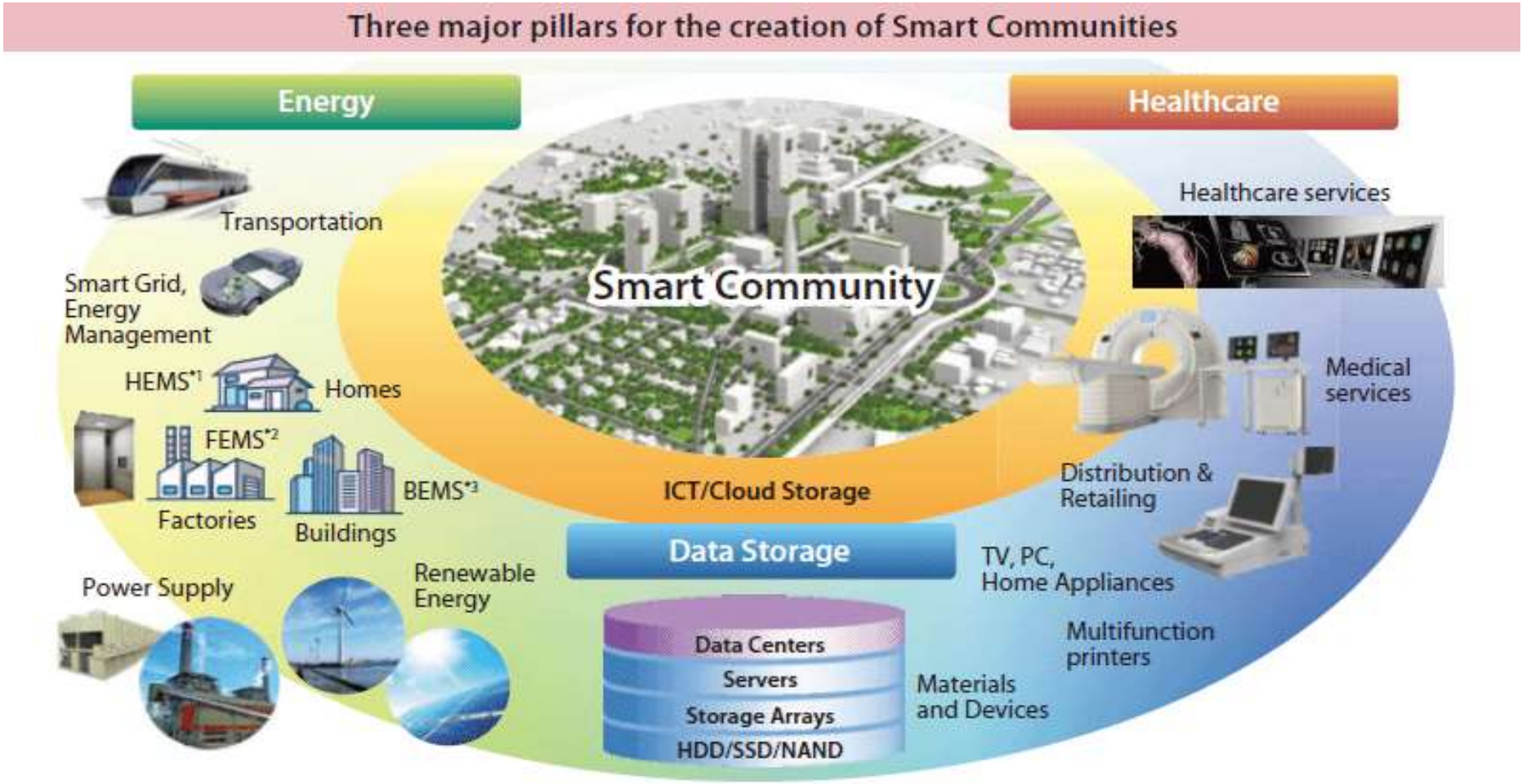
1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

- Do chúng ta sống trong "thế giới kết nối" với mức độ ngày càng "sâu"
- Ngày càng có nhiều nguy cơ, đe dọa mất an toàn thông tin, hệ thống, mạng.

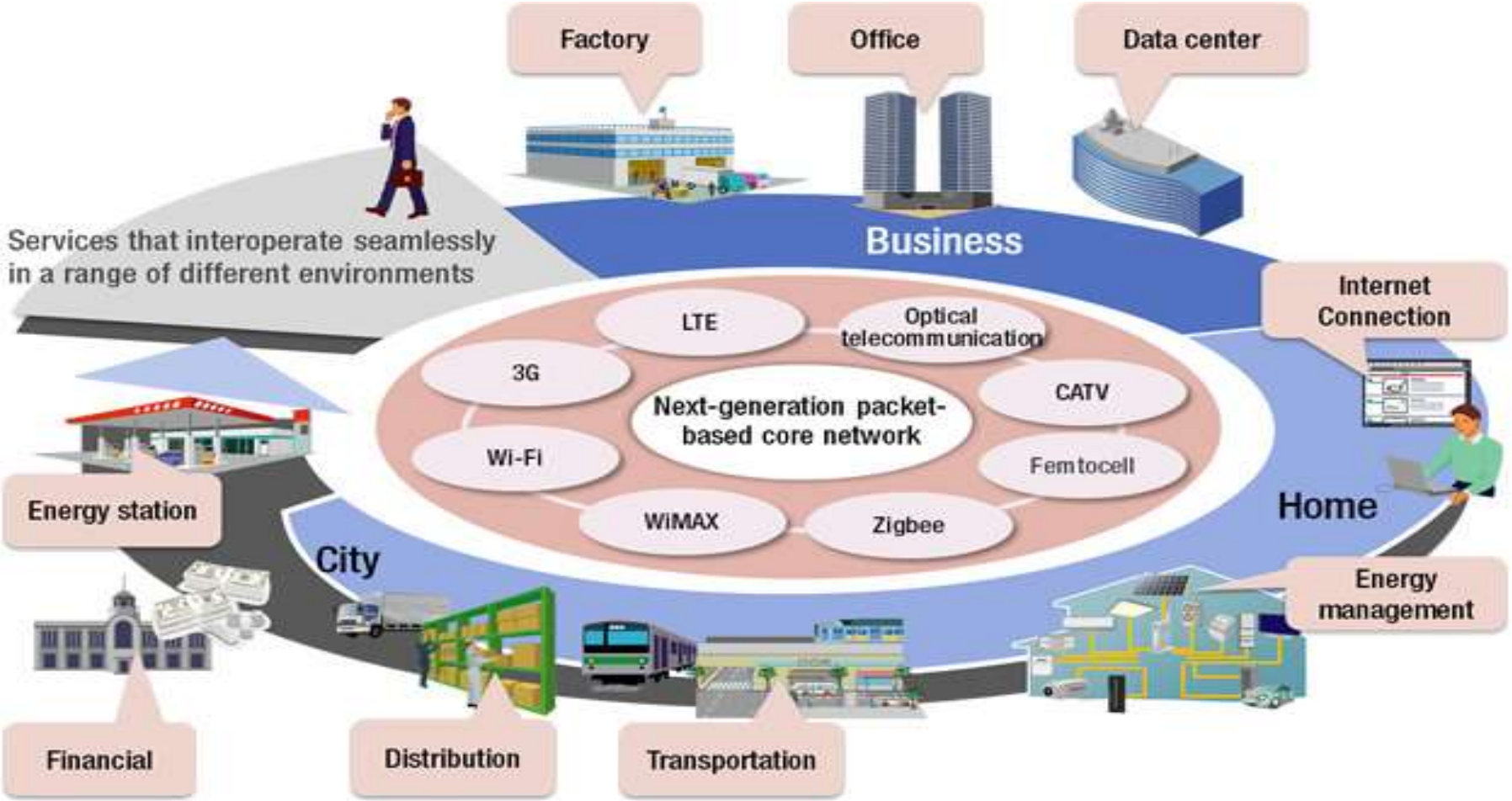
1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

- Do chúng ta sống trong "thế giới kết nối":
  - Mọi thiết bị tính toán & truyền thông đều có kết nối Internet;
  - Các hệ thống kết nối "sâu và rộng" ngày càng phổ biến:
    - Smart community (cộng đồng thông minh)
    - Smart city (thành phố thông minh)
    - Smart home (ngôi nhà thông minh),…
  - Các khái niệm kết nối mọi vật, kết nối tất cả trở nên 'nóng':
    - IoT: Internet of Things
    - IoE: Internet of Everything.
  - Các hệ thống không có kết nối khả năng sử dụng hạn chế.

1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

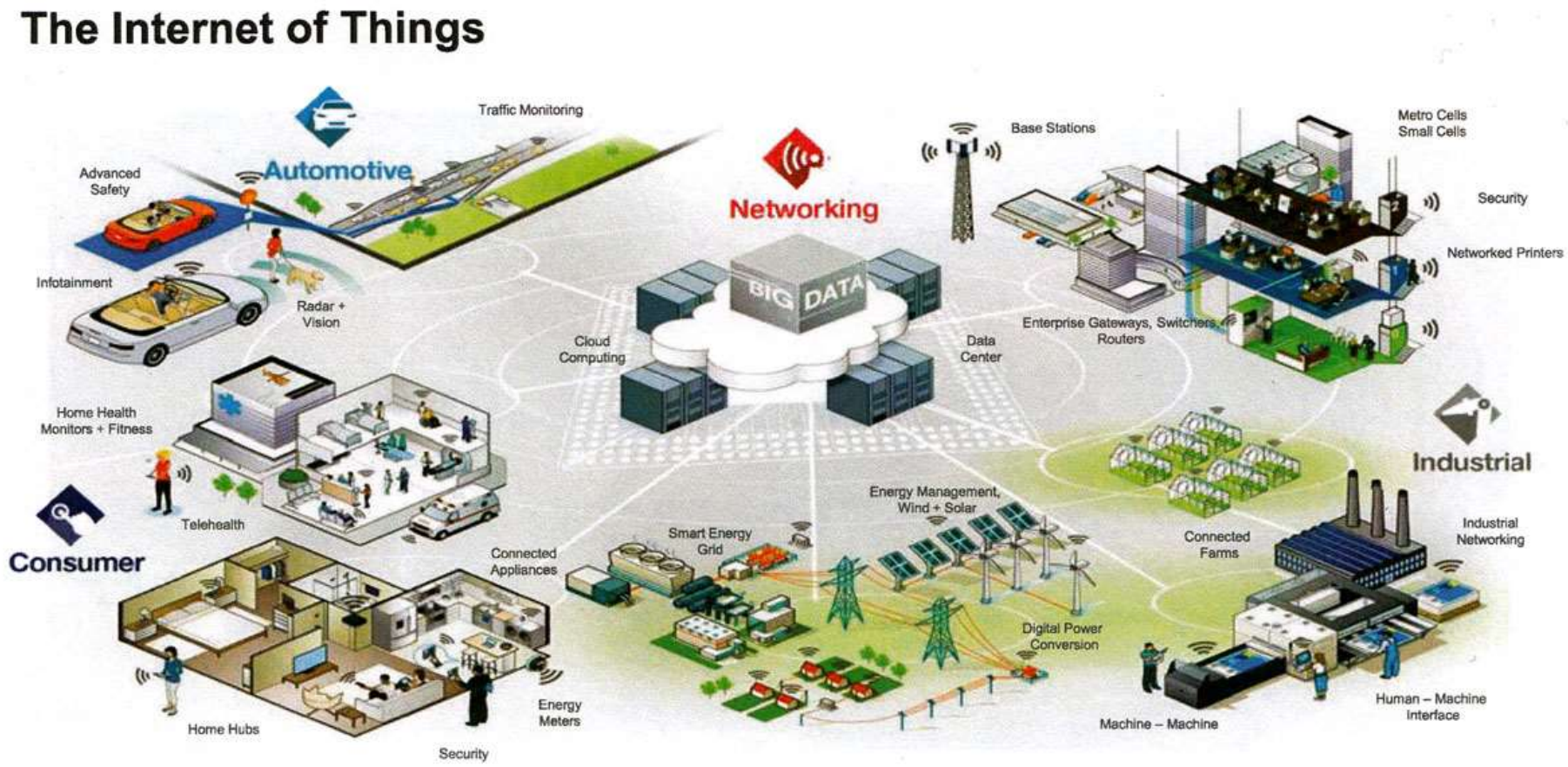


1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin



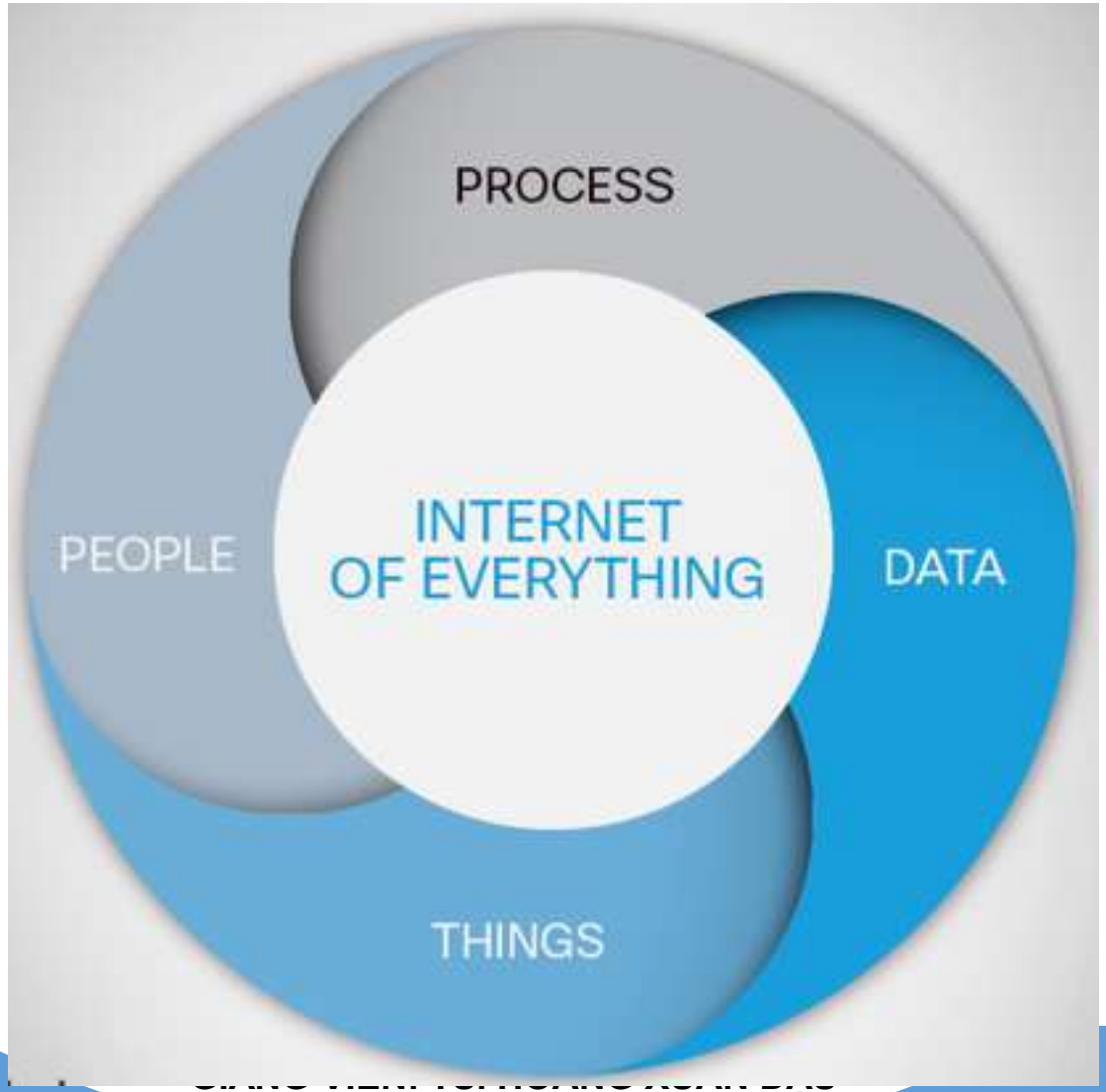
1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

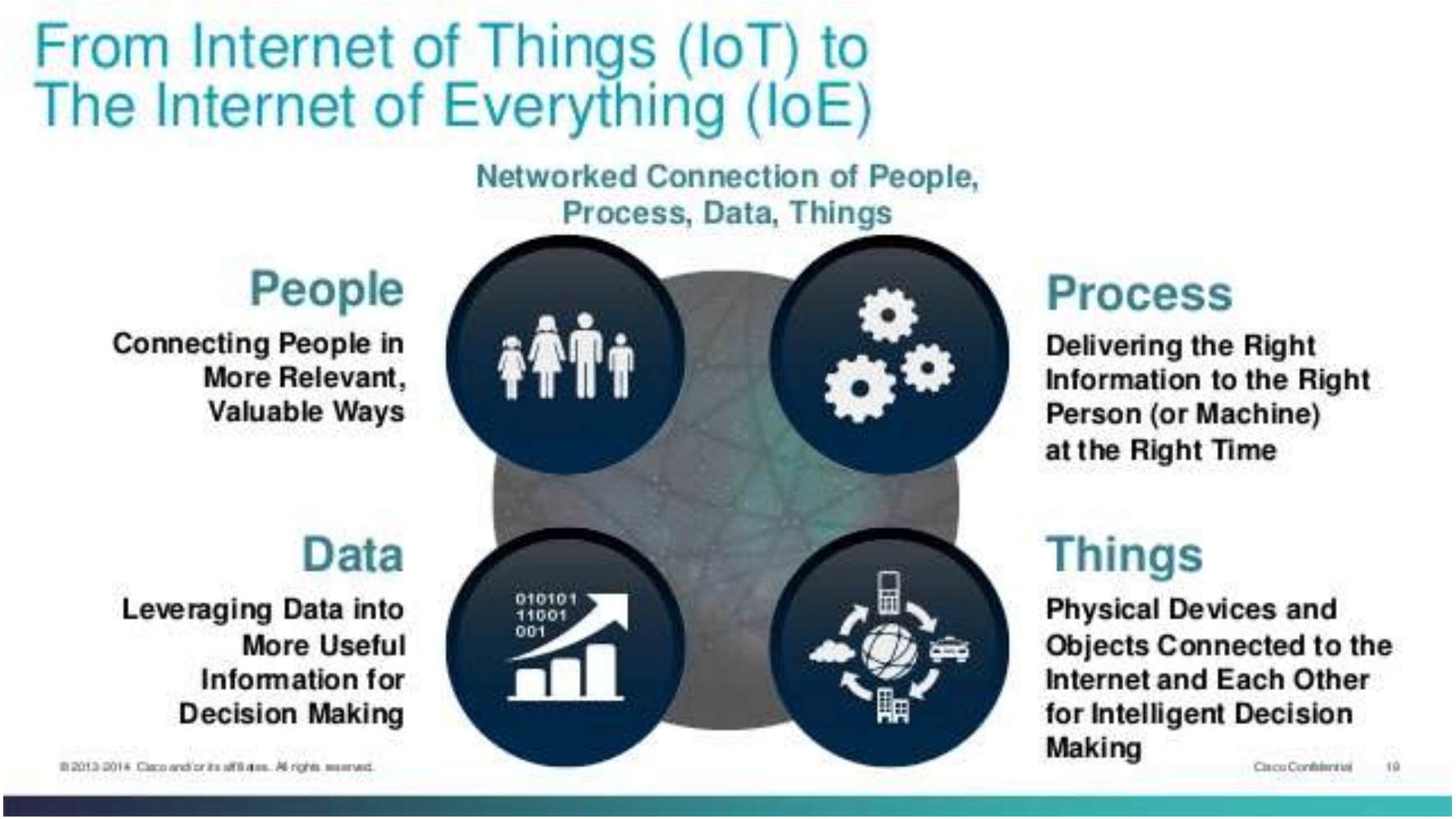


1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin



1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

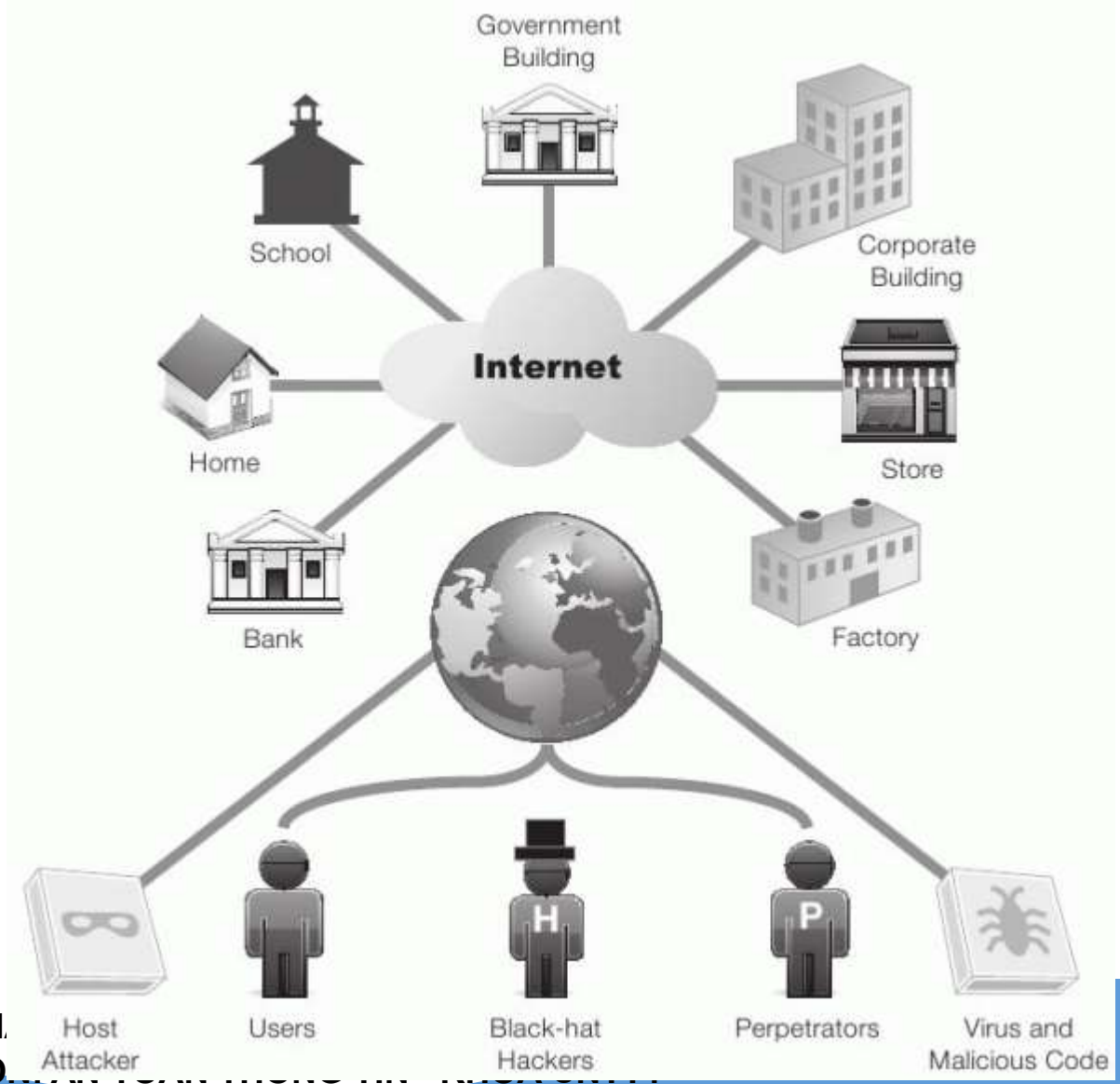


1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

- Ngày càng có nhiều nguy cơ, đe dọa mất an toàn thông tin, hệ thống, mạng:
  - Bị tấn công từ tin tặc
  - Bị tấn công hoặc lạm dụng từ người dùng
  - Lây nhiễm các phần mềm độc hại (vi rút, sâu,...)
  - Nguy cơ bị nghe trộm, đánh cắp và sửa đổi thông tin
  - Lỗi hoặc các khiếm khuyết phần cứng, phần mềm.

1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

Thế giới kết nối với nhiều nguy cơ và đe dọa



1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

Các mối đe dọa và nguy cơ thường trực: tin tặc (hackers) và các phần mềm độc hại (viruses, worms, trojans)

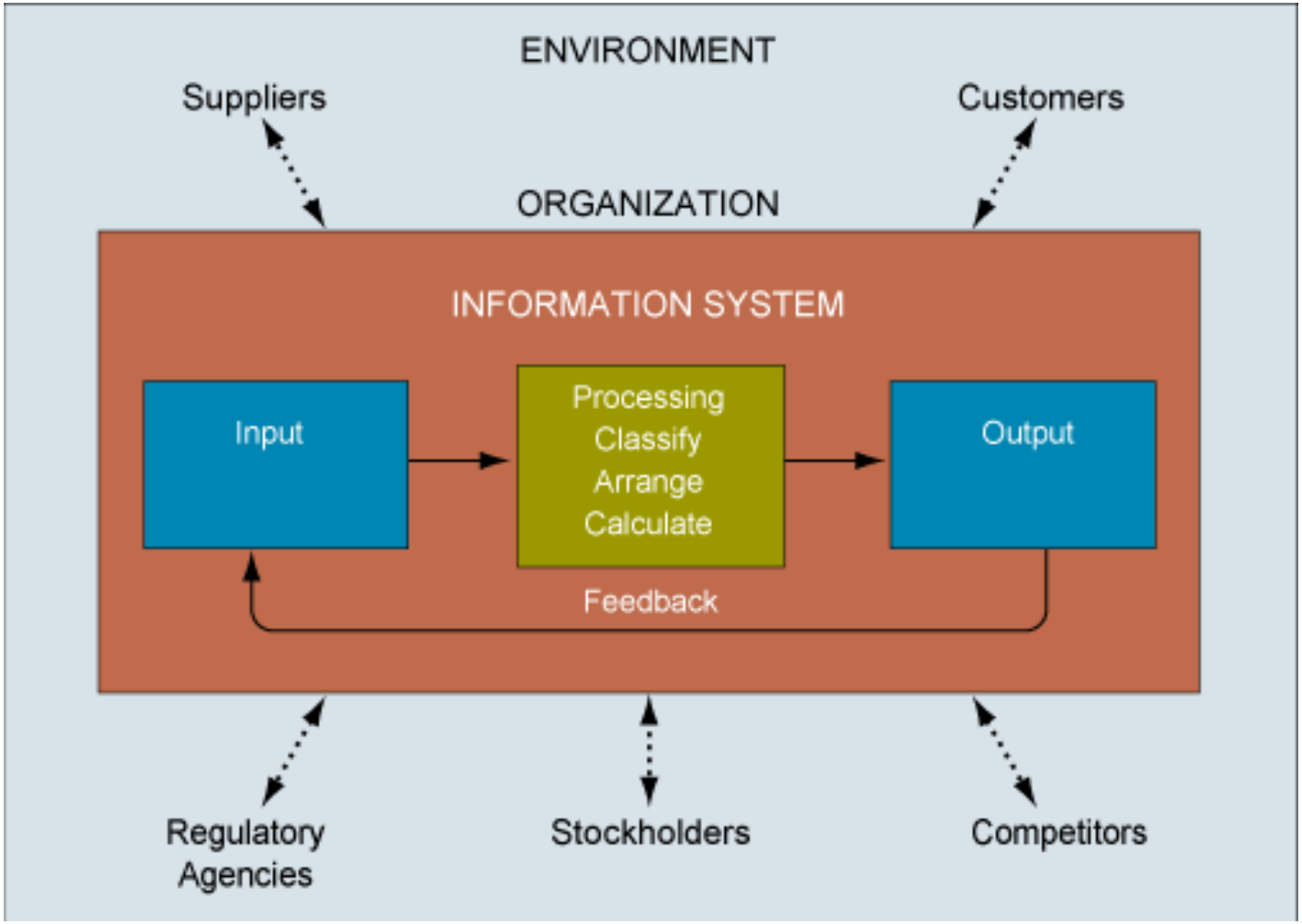
1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

❖ Hệ thống thông tin là gì?

- Hệ thống thông tin (IS – Information System) là một hệ thống tích hợp các thành phần nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin và chuyển giao thông tin, tri thức và các sản phẩm số;
- Các doanh nghiệp và các tổ chức sử dụng các hệ thống thông tin (HTTT) để thực hiện và quản lý các hoạt động:
  - Tương tác với khác khàng;
  - Tương tác với các nhà cung cấp;
  - Tương tác với các cơ quan chính quyền;
  - Quảng bá thương hiệu và sản phẩm;
  - Cạnh tranh với các đối thủ trên thị trường.

1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

- Hệ thống thông tin là gì?

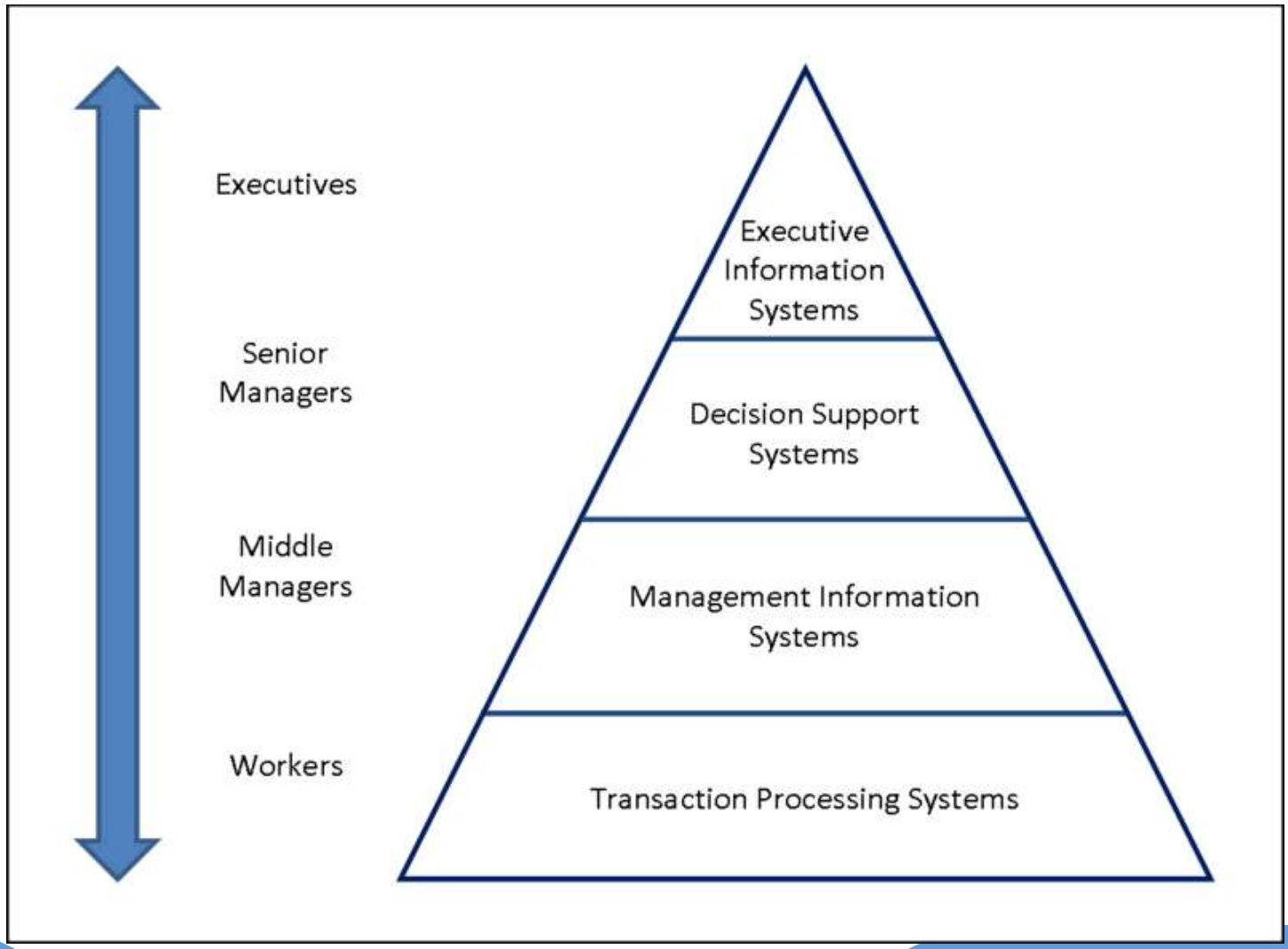


1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

- Các loại hệ thống thông tin (mô hình tháp): gồm 4 loại theo đối tượng sử dụng:
  - Hệ thống xử lý giao dịch (Transactional Processing Systems) với người sử dụng là các nhân viên (Workers);
  - Hệ thống thông tin quản lý (Management Information Systems) với người sử dụng là các quản lý bộ phận (Middle Managers);
  - Hệ thống trợ giúp ra quyết định (Decision Support Systems) với người sử dụng là các quản lý cao cấp (Senior Managers);
  - Hệ thống thông tin điều hành (Executive Information Systems) với người sử dụng là các Giám đốc điều hành (Executives).

1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

- Các loại hệ thống thông tin (mô hình tháp)



1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

- Một số hệ thống thông tin điển hình:
  - Các kho dữ liệu (data warehouses)
  - Các hệ lập kế hoạch nguồn lực doanh nghiệp (enterprise resource planning)
  - Các hệ thống thông tin doanh nghiệp (enterprise systems)
  - Các hệ chuyên gia (expert systems)
  - Các máy tìm kiếm (search engines)
  - Các hệ thống thông tin địa lý (geographic information system)
  - Các hệ thống thông tin toàn cầu (global information system)
  - Các hệ tự động hóa văn phòng (office automation).

1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

- Một hệ thống thông tin dựa trên máy tính (Computer-Based Information System) là một hệ thống thông tin sử dụng công nghệ máy tính để thực thi các nhiệm vụ.
- Các thành phần của hệ thống thông tin dựa trên máy tính:
  - Hardware: phần cứng để thu thập, lưu trữ, xử lý và biểu diễn dữ liệu
  - Software: các phần mềm chạy trên phần cứng để xử lý dữ liệu
  - Databases: lưu trữ dữ liệu
  - Networks: hệ thống truyền dẫn thông tin/dữ liệu
  - Procedures: tập hợp các lệnh kết hợp các bộ phận nêu trên để xử lý dữ liệu, đưa ra kết quả mong muốn.

1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

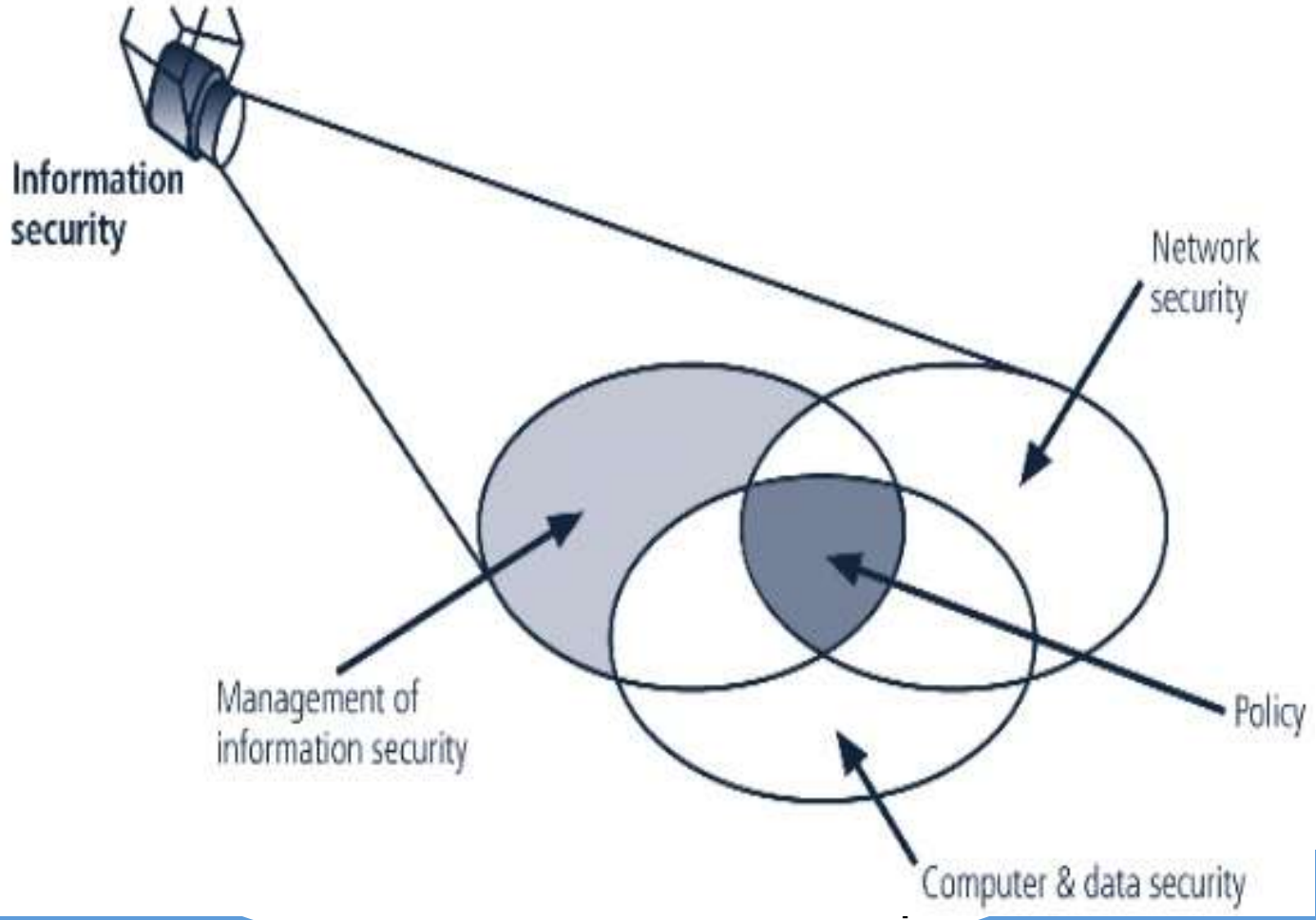
- An toàn thông tin (Information Security) là gì?
  - An toàn thông tin là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép.
- Hai lĩnh vực chính của an toàn thông tin (ATTT):
  - An toàn công nghệ thông tin (IT Security):
    - Đôi khi còn gọi là an toàn máy tính (Computer Security) là ATTT áp dụng cho các hệ thống công nghệ;
    - Các hệ thống công nghệ thông tin của 1 tổ chức cần được đảm bảo an toàn khỏi các tấn công mạng.
  - Đảm bảo thông tin (Information Assurance):
    - Đảm bảo thông tin không bị mất khi xảy ra các sự cố (thiên tai, hỏng hóc hệ thống, trộm cắp, phá hoại,…);
    - Thường sử dụng kỹ thuật tạo dự phòng ngoại vi (offsite backup).

1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

- Các thành phần của ATTT:
  - An toàn máy tính và dữ liệu (Computer and data security)
  - An ninh mạng (Network security)
  - Quản lý ATTT (Management of information security)
  - Chính sách ATTT (Policy)

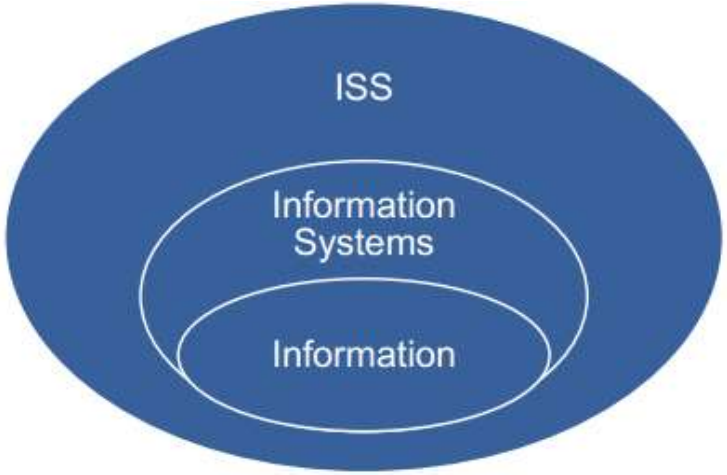
1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

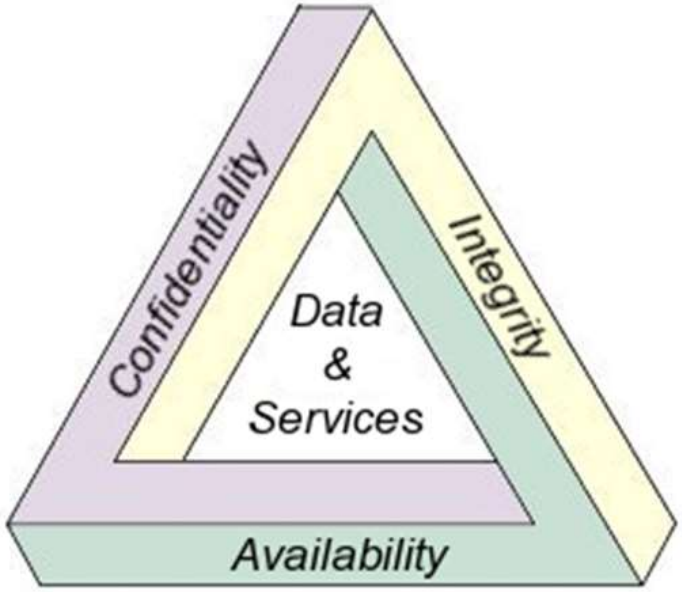
❖ Các thành phần của ATTT:



1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

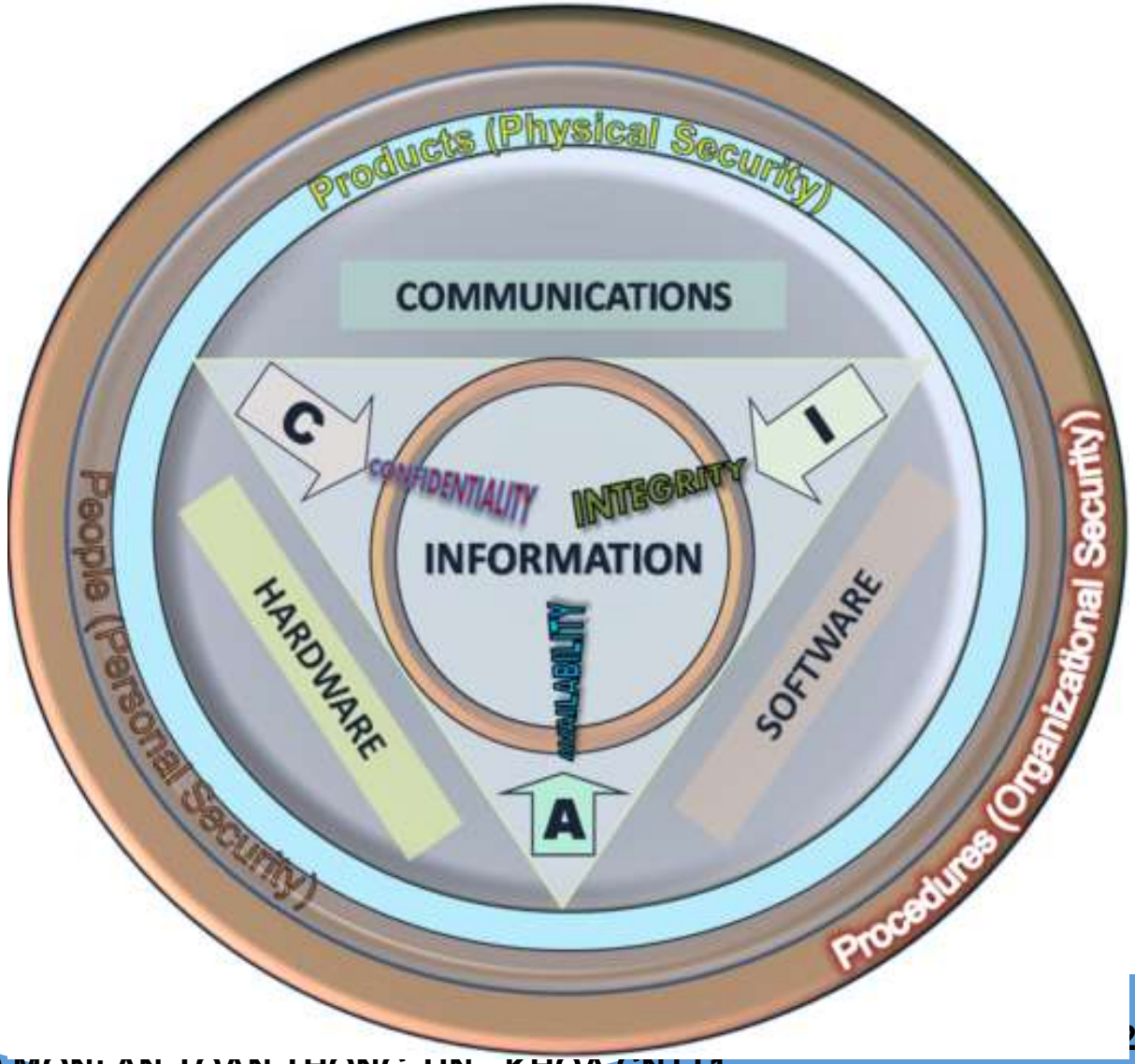
- An toàn hệ thống thông tin (ISS - Information Systems Security): là việc đảm bảo các thuộc tính an ninh an toàn của hệ thống thông tin:
  - Bí mật (Confidentiality)
  - Toàn vẹn (Integrity)
  - Sẵn dùng (Availability)





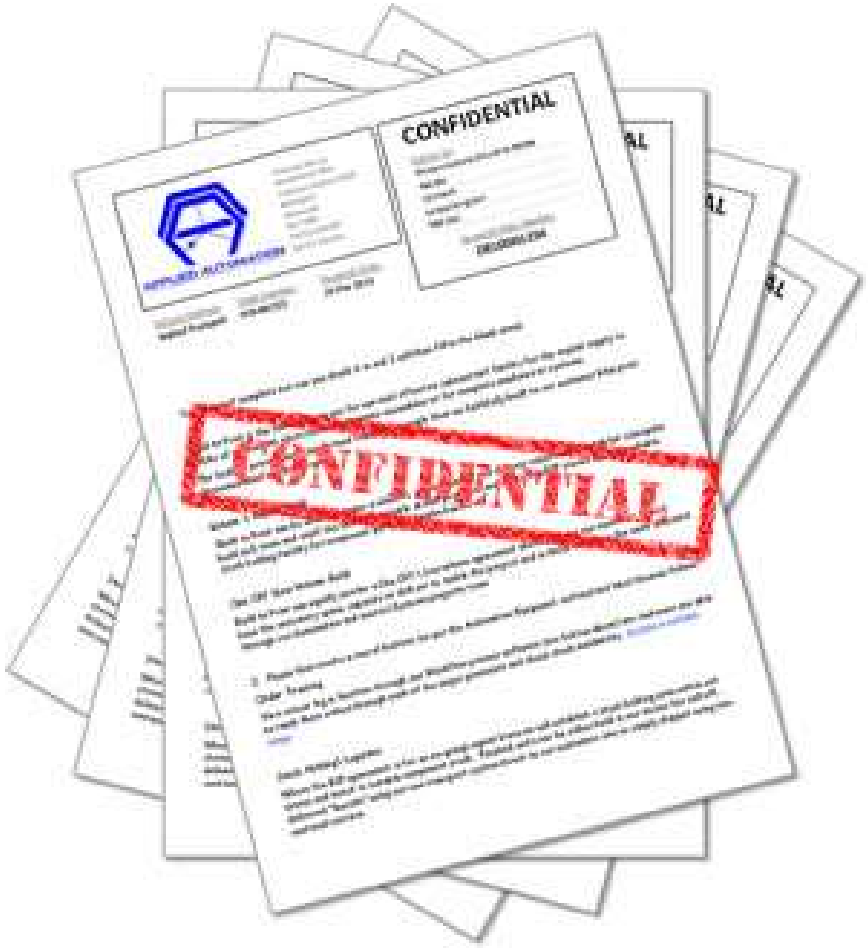
1.1 Giới thiệu về ATTT và an toàn hệ thống thông tin

- An toàn hệ thống thông tin (ISS)



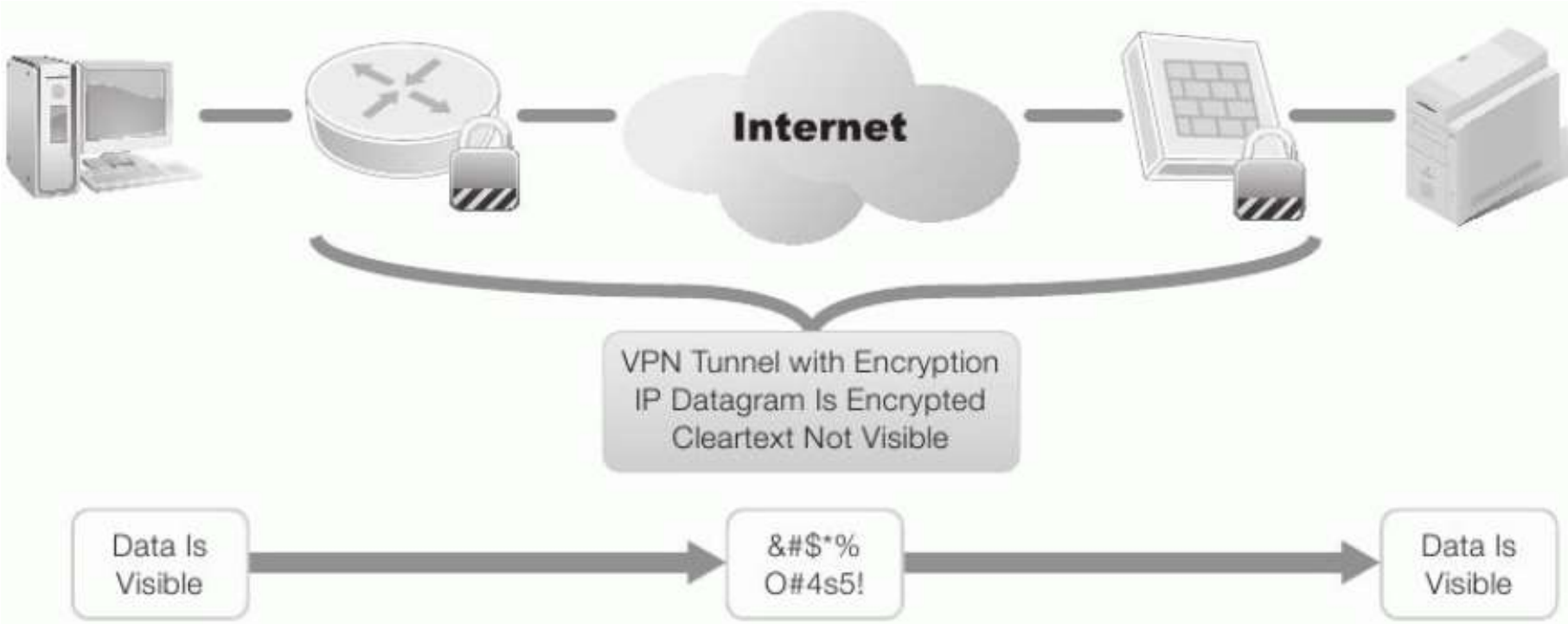
1.2 Các yêu cầu đảm bảo an toàn HTTT

- Tính bí mật (Confidentiality): chỉ người dùng có thẩm quyền mới được truy nhập thông tin.
- Các thông tin bí mật có thể gồm:
  - Dữ liệu riêng của cá nhân;
  - Các thông tin thuộc quyền sở hữu trí tuệ của các doanh nghiệp hay các cơ quan/tổ chức;
  - Các thông tin có liên quan đến an ninh quốc gia.



1.2 Các yêu cầu đảm bảo an toàn HTTT

❖ Tính bí mật được đảm bảo bằng kênh mã hóa VPN

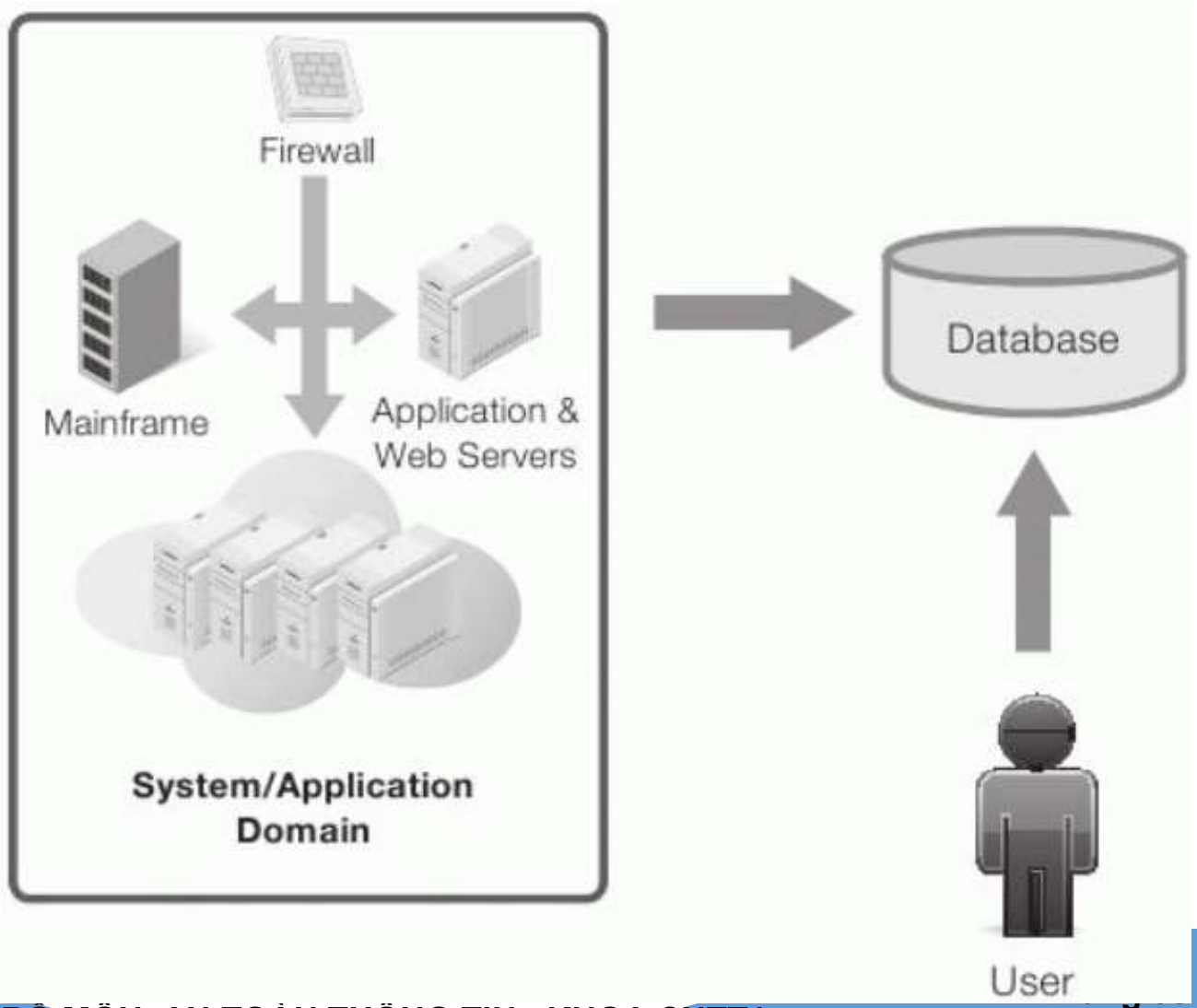


1.2 Các yêu cầu đảm bảo an toàn HTTT

- Tính toàn vẹn (Integrity): thông tin chỉ có thể được sửa đổi bởi những người dùng có thẩm quyền.
- Tính toàn vẹn liên quan đến tính hợp lệ (validity) và chính xác (accuracy) của dữ liệu.
  - Trong nhiều tổ chức, thông tin có giá trị rất lớn, như bản quyền phần mềm, bản quyền âm nhạc, bản quyền phát minh, sáng chế;
  - Mọi thay đổi không có thẩm quyền có thể ảnh hưởng rất nhiều đến giá trị của thông tin.
- Dữ liệu là toàn vẹn nếu:
  - Dữ liệu không bị thay đổi;
  - Dữ liệu hợp lệ;
  - Dữ liệu chính xác.

1.2 Các yêu cầu đảm bảo an toàn HTTT

- Tính toàn vẹn của hệ thống thông tin: thông tin chỉ được sửa đổi bởi người dùng có thẩm quyền.

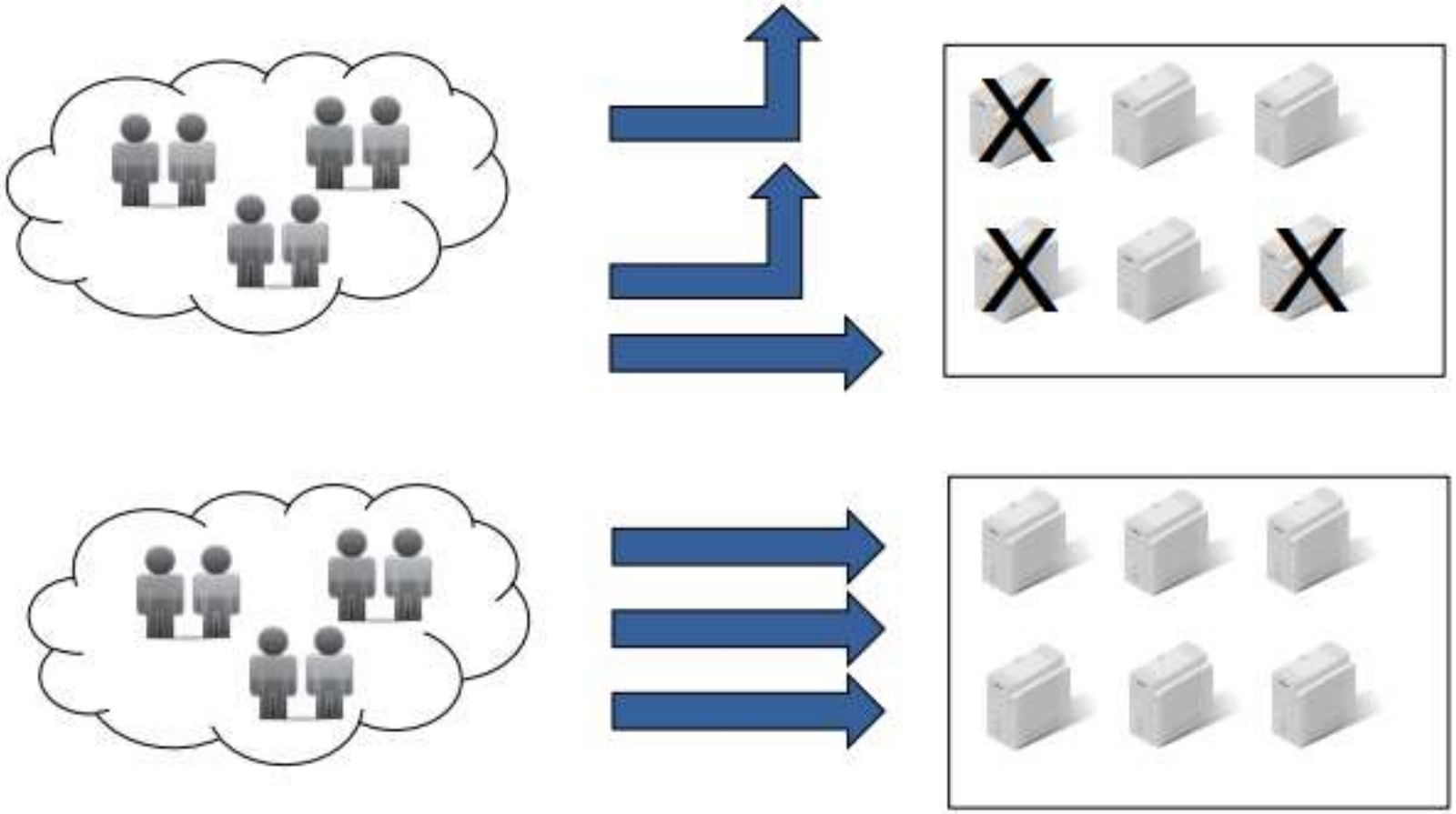


1.2 Các yêu cầu đảm bảo an toàn HTTT

- Tính sẵn dùng (Availability): thông tin có thể truy nhập bởi người dùng hợp pháp bất cứ khi nào họ có yêu cầu.
- Tính sẵn dùng có thể được đo bằng các yếu tố:
  - Thời gian cung cấp dịch vụ (Uptime);
  - Thời gian ngừng cung cấp dịch vụ (Downtime);
  - Tỷ lệ phục vụ: A = (Uptime)/(Uptime + Downtime);
  - Thời gian trung bình giữa các sự cố;
  - Thời gian trung bình ngừng để sửa chữa;
  - Thời gian khôi phục sau sự cố.

1.2 Các yêu cầu đảm bảo an toàn HTTT

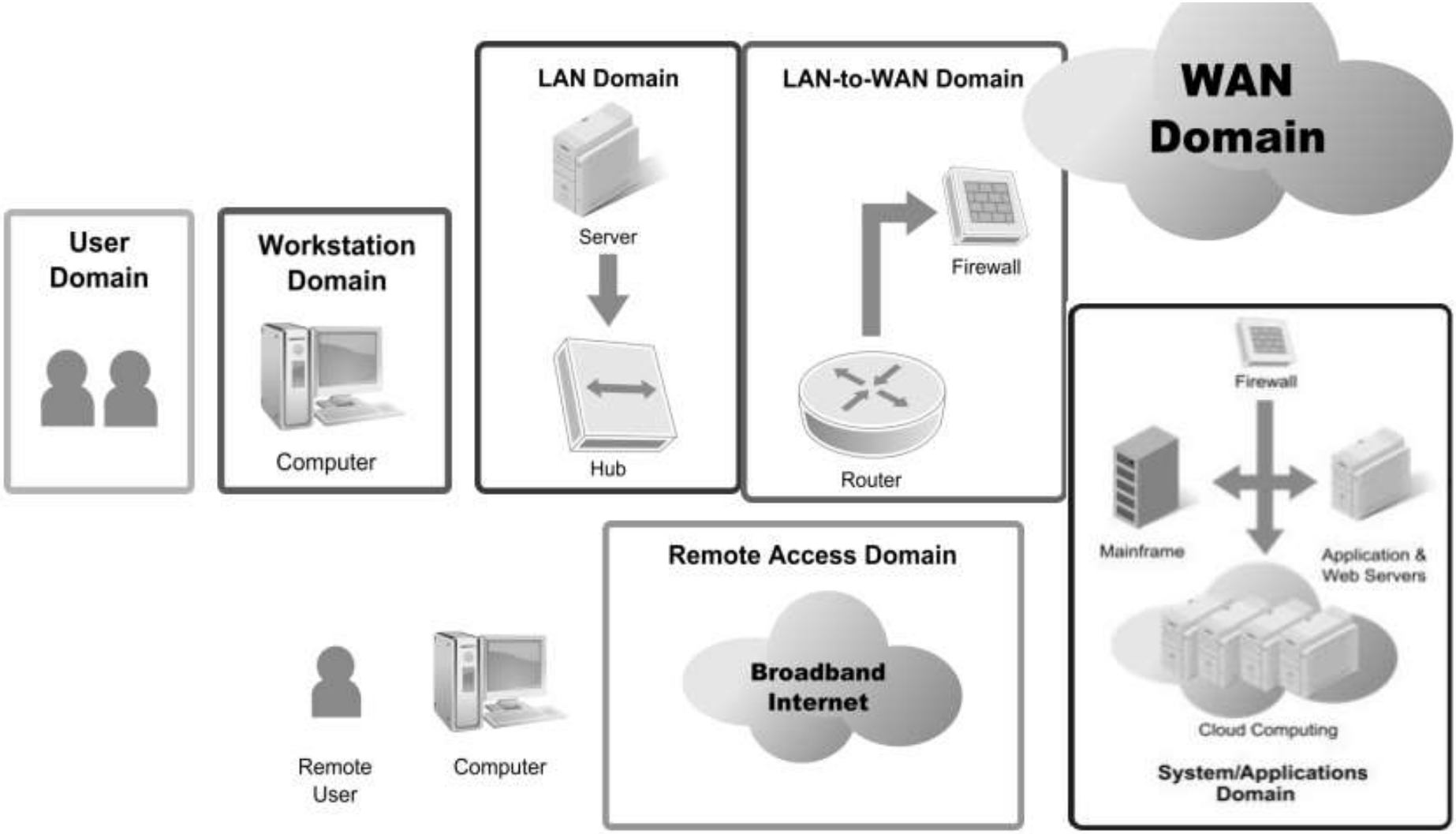
❖ Tính sẵn dùng



1.3 Bảy vùng trong cơ sở hạ tầng CNTT và các mối đe dọa

- Vùng người dùng (User domain)
- Vùng máy trạm (Workstation domain)
- Vùng mạng LAN (LAN domain)
- Vùng LAN-to-WAN (LAN-to-WAN domain)
- Vùng WAN (WAN domain)
- Vùng truy nhập từ xa (Remote Access domain)
- Vùng hệ thống/ứng dụng (Systems/Applications domain)

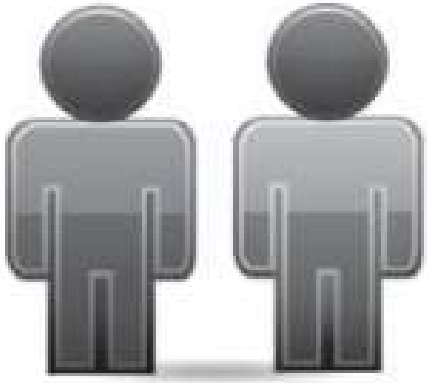
1.3 Bảy vùng trong cơ sở hạ tầng CNTT và các mối đe dọa



1.3 Bảy vùng trong cơ sở hạ tầng CNTT và các mối đe dọa

❖ Các đe dọa (threats) với vùng người dùng:

- Thiếu ý thức về vấn đề an ninh an toàn
- Coi nhẹ các chính sách an ninh an toàn
- Vi phạm chính sách an ninh an toàn
- Đưa CD/DVD/USB với các files cá nhân vào hệ thống
- Tải ảnh, âm nhạc, video
- Phá hoại dữ liệu, ứng dụng và hệ thống
- Tấn công phá hoại từ các nhân viên bất mãn
- Nhân viên có thể tống tiền hoặc chiếm đoạt thông tin quan trọng.



1.3 Bảy vùng trong cơ sở hạ tầng CNTT và các mối đe dọa

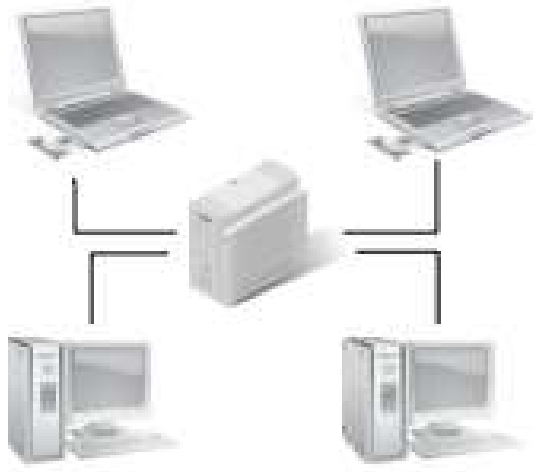
❖ Các đe dọa (threats) với vùng máy trạm:

- Truy nhập trái phép vào máy trạm
- Truy nhập trái phép vào hệ thống, ứng dụng và dữ liệu
- Các lỗ hổng an ninh trong hệ điều hành máy trạm
- Các lỗ hổng an ninh trong các phần mềm ứng dụng máy trạm
- Các hiểm họa từ virus, mã độc và các phần mềm độc hại
- Người dùng đưa CD/DVD/USB với các files cá nhân vào hệ thống
- Người dùng tải ảnh, âm nhạc, video.

1.3 Bảy vùng trong cơ sở hạ tầng CNTT và các mối đe dọa

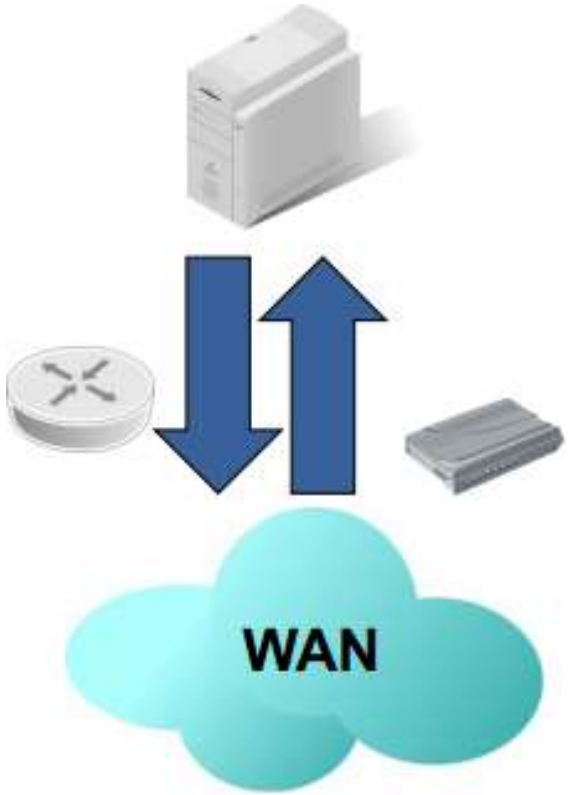
❖ Các đe dọa (threats) với vùng LAN:

- Truy nhập trái phép vào mạng LAN vật lý
- Truy nhập trái phép vào hệ thống, ứng dụng và dữ liệu
- Các lỗ hổng an ninh trong hệ điều hành máy chủ
- Các lỗ hổng an ninh trong các phần mềm ứng dụng máy chủ
- Nguy cơ từ người dùng giả mạo trong mạng WLAN
- Tính bí mật dữ liệu trong mạng WLAN có thể bị đe dọa
- Các hướng dẫn và chuẩn cấu hình cho máy chủ LAN chưa được tuân thủ.



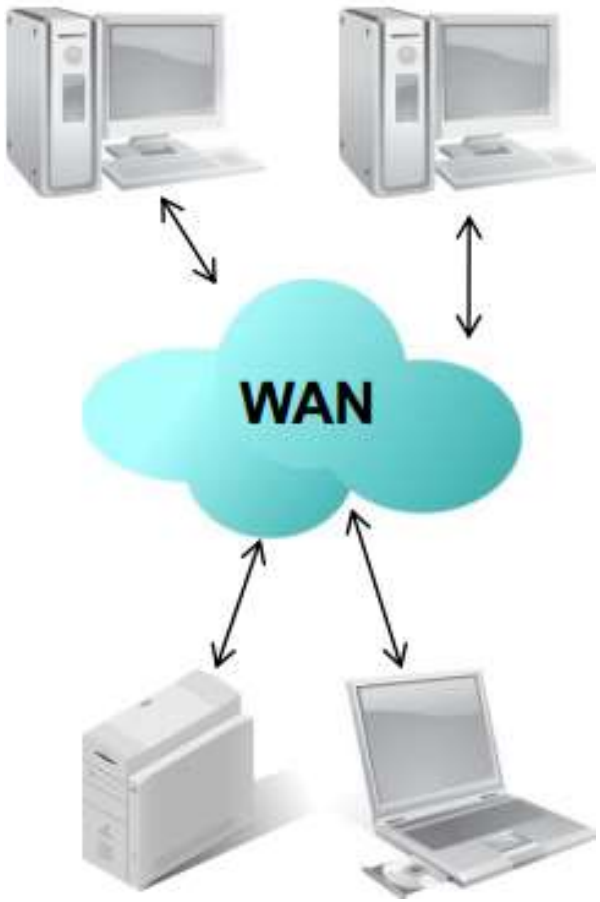
1.3 Bảy vùng trong cơ sở hạ tầng CNTT và các mối đe dọa

- Các đe dọa (threats) với vùng LAN-to-WAN:
  - Thăm dò và rà quét trái phép các cổng dịch vụ
  - Truy nhập trái phép
  - Lỗ hổng an ninh trong các bộ định tuyến, tường lửa và các thiết bị mạng khác
  - Người dụng cục bộ (trong LAN) có thể tải các file không xác định nội dung từ các nguồn không xác định.



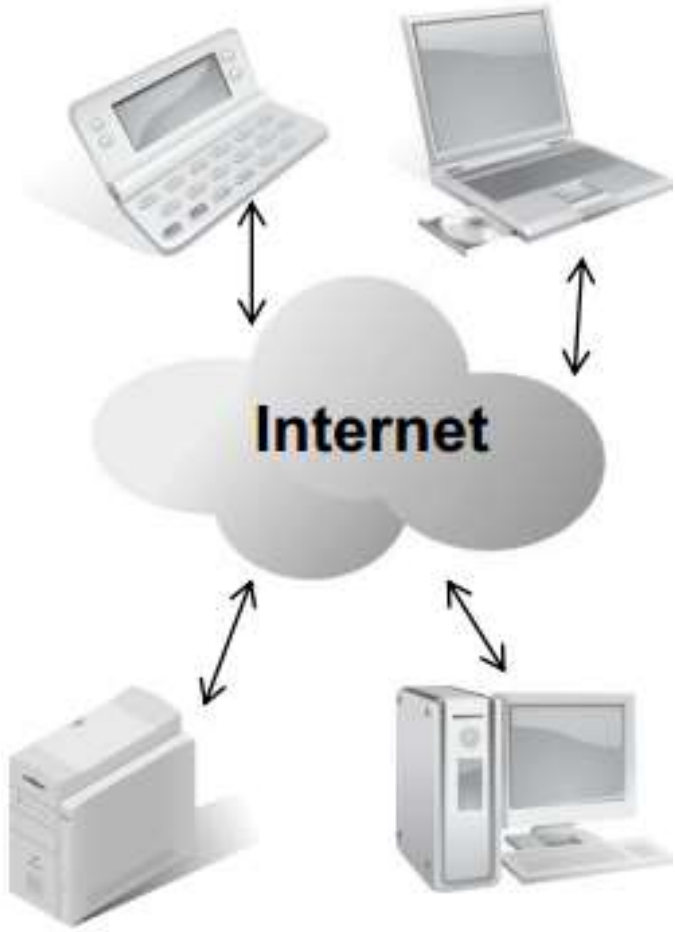
1.3 Bảy vùng trong cơ sở hạ tầng CNTT và các mối đe dọa

- Các đe dọa (threats) với vùng WAN:
  - Rủi ro từ việc dữ liệu có thể được truy nhập trong môi trường công cộng và mở
  - Hầu hết dữ liệu được truyền dưới dạng rõ (cleartext/plaintext)
  - Dễ bị nghe trộm
  - Dễ bị tấn công phá hoại
  - Dễ bị tấn công từ chối dịch vụ (DoS) và từ chối dịch vụ phân tán (DDoS)
  - Kẻ tấn công có thể tự do, dễ dàng gửi email có đính kèm virus, sâu và các phần mềm độc hại.



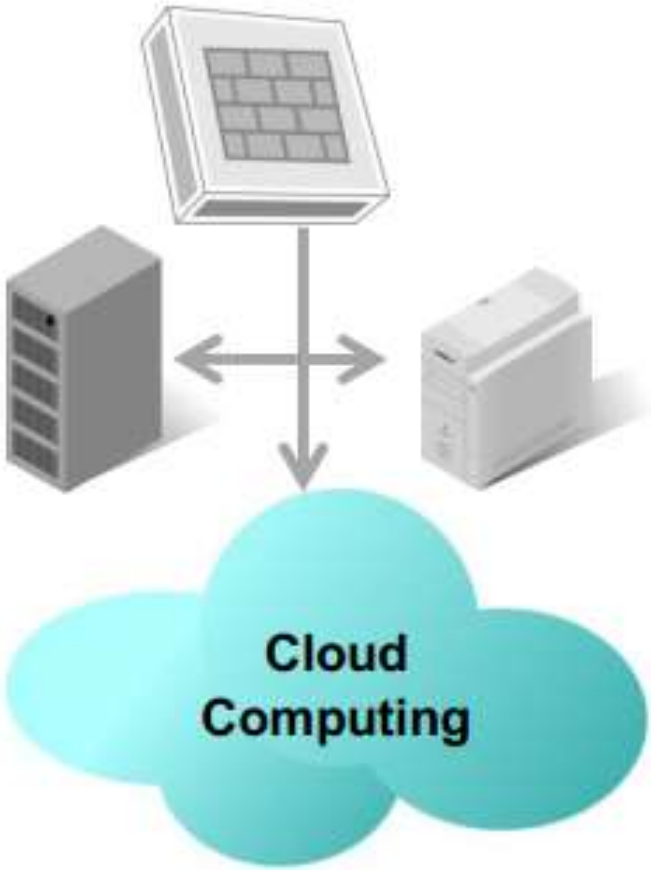
1.3 Bảy vùng trong cơ sở hạ tầng CNTT và các mối đe dọa

- Các đe dọa (threats) với vùng truy nhập từ xa:
  - Tấn công kiểu vét cạn (brute force) vào tên người dùng và mật khẩu
  - Tấn công vào hệ thống đăng nhập và điều khiển truy cập
  - Truy nhập trái phép vào hệ thống CNTT, ứng dụng và dữ liệu
  - Thông tin bí mật có thể bị đánh cắp từ xa
  - Dò rỉ dữ liệu do vi phạm các tiêu chuẩn phân loại dữ liệu.



1.3 Bảy vùng trong cơ sở hạ tầng CNTT và các mối đe dọa

- Các đe dọa (threats) với vùng hệ thống/ứng dụng:
  - Truy nhập trái phép đến trung tâm dữ liệu, phòng máy hoặc tủ cáp
  - Khó khăn trong quản lý các máy chủ yêu cầu tính sẵn dùng cao
  - Lỗ hổng trong quản lý các phần mềm ứng dụng của hệ điều hành máy chủ
  - Các vấn đề an ninh trong các môi trường ảo của điện toán đám mây
  - Vấn đề hỏng hóc hoặc mất dữ liệu.

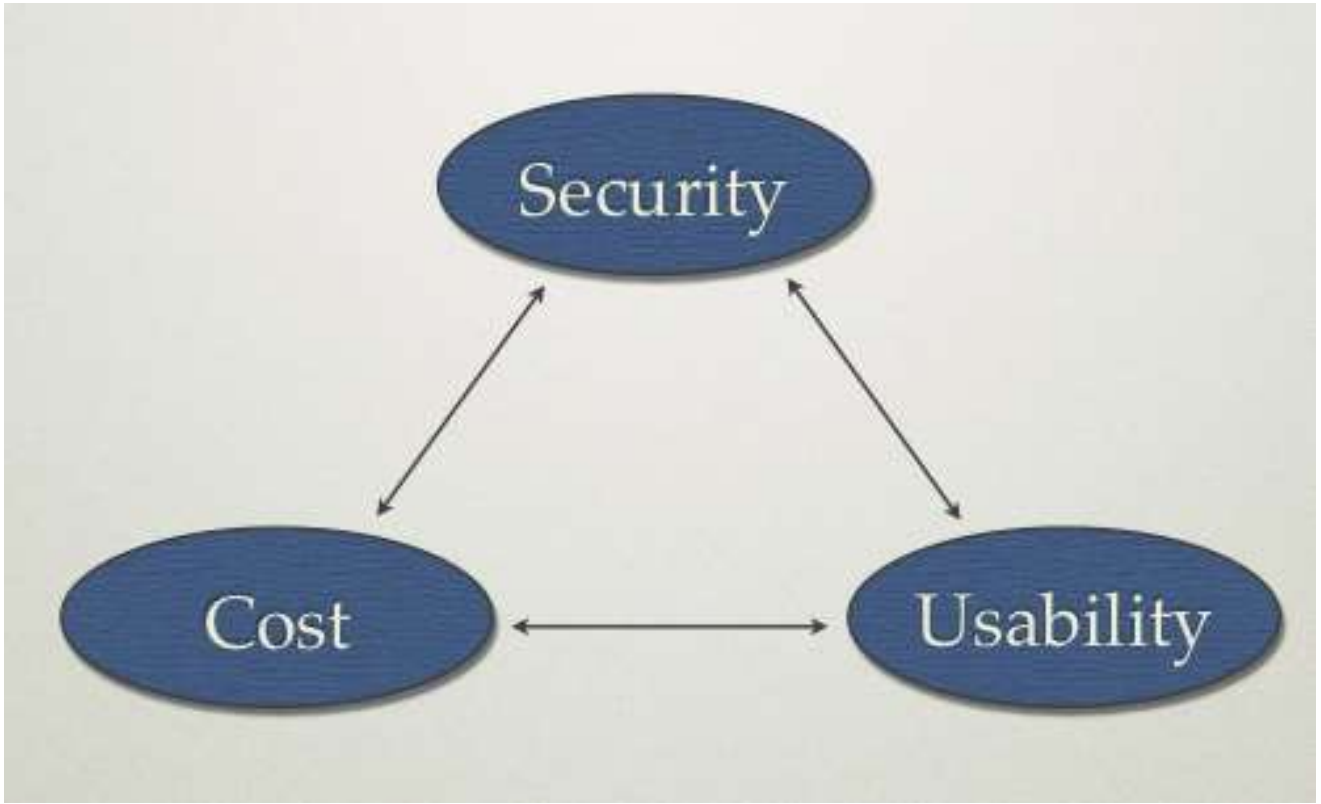


1.4 Mô hình tổng quát đảm bảo an toàn HTTT

- Nguyên tắc đảm bảo an toàn thông tin, hệ thống và mạng:
  - Phòng vệ nhiều lớp có chiều sâu (Defence in Depth): tạo ra nhiều lớp bảo vệ, kết hợp tính năng tác dụng của mỗi lớp để đảm bảo an toàn tối đa cho thông tin, hệ thống và mạng.
  - Một lớp, một công cụ phòng vệ thường không đảm bảo an toàn.
  - Không tồn tại HTTT an toàn tuyệt đối
    - Thường HTTT an toàn tuyệt đối là hệ thống đóng kín và không hoặc ít có giá trị sử dụng.
    - Cần cân bằng giữa an toàn, tính hữu dụng và chi phí đảm bảo an toàn.

1.4 Mô hình tổng quát đảm bảo an toàn HTTT

- Cần cân bằng giữa Usability (Tính hữu dụng), Cost (chi phí) và Security (an toàn)

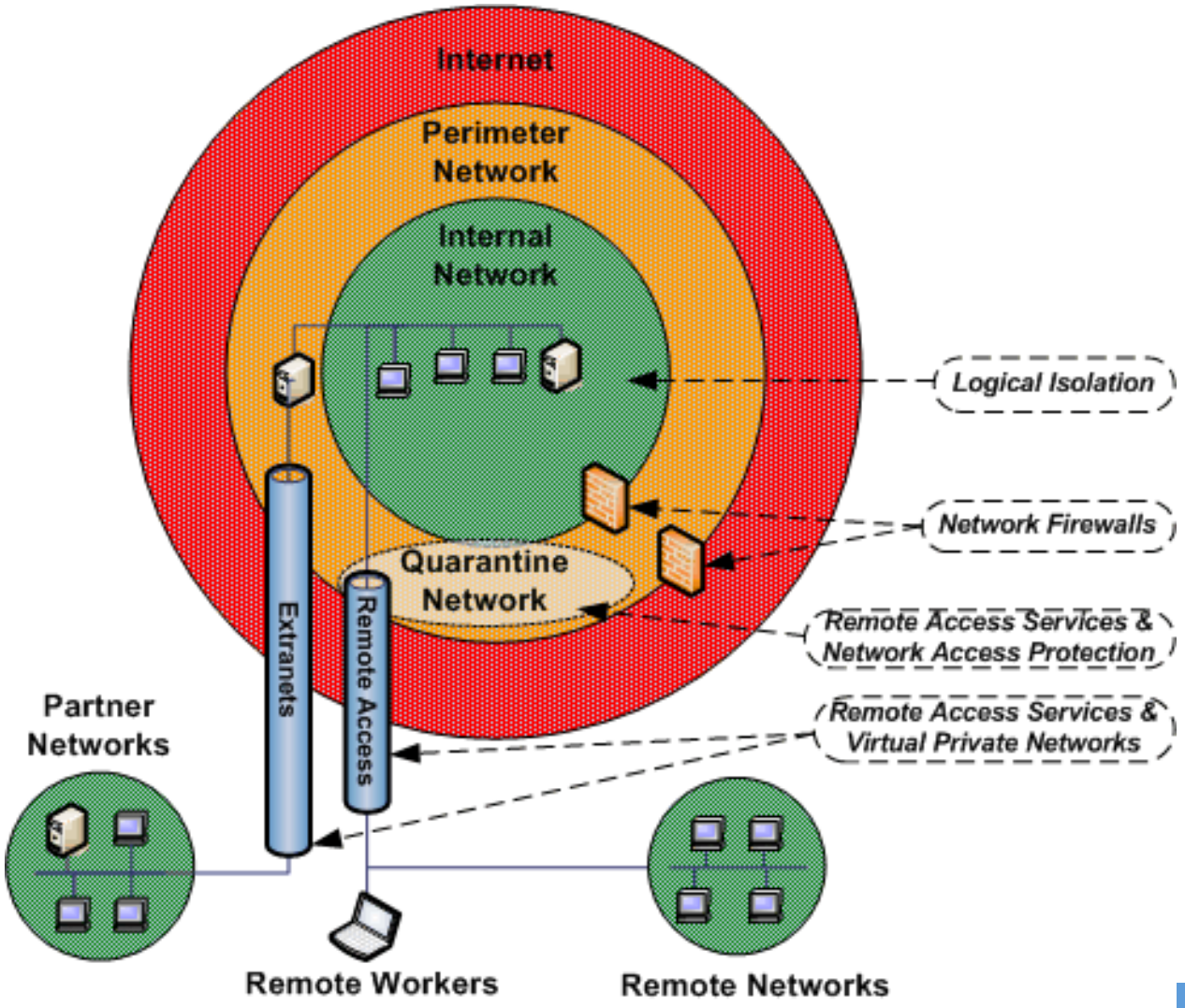


1.4 Mô hình tổng quát đảm bảo an toàn HTTT

❖ Mô hình Layered Security Model hoặc Defence in Depth

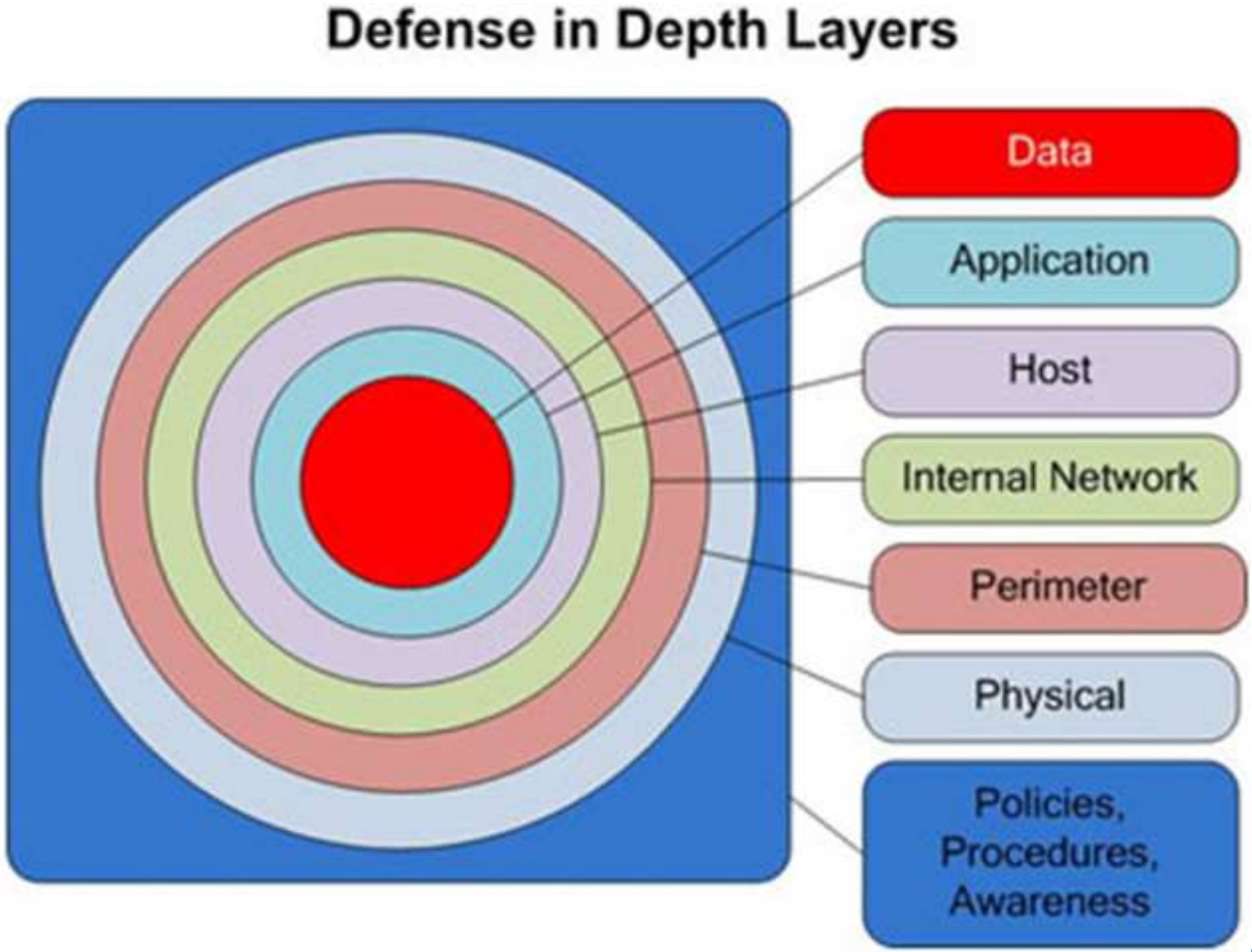
1.4 Mô hình tổng quát đảm bảo an toàn HTTT

- Mô hình Layered Security Model hoặc Defence in Depth



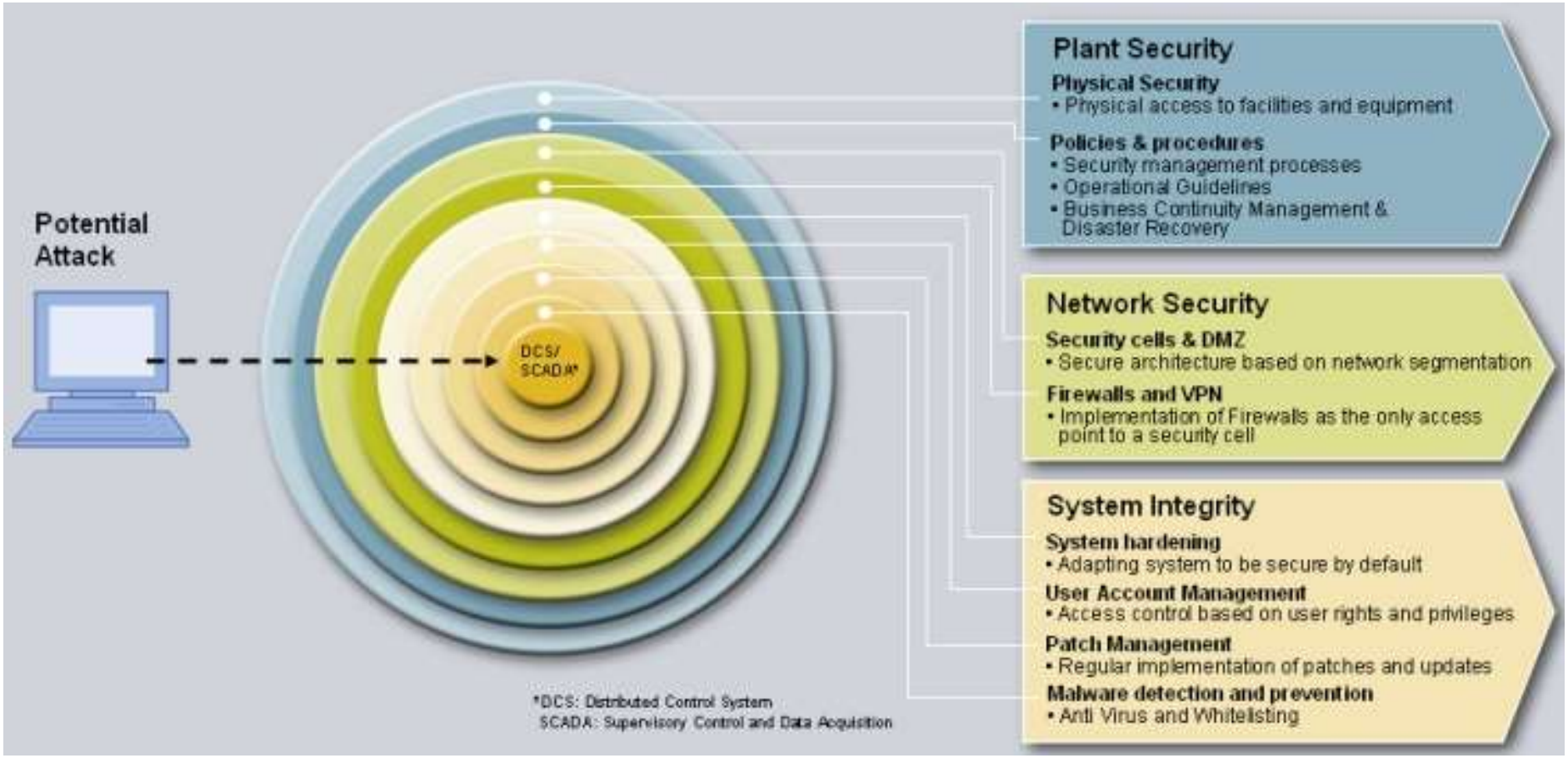
1.4 Mô hình tổng quát đảm bảo an toàn HTTT

- Mô hình Layered Security Model hoặc Defence in Depth



1.4 Mô hình tổng quát đảm bảo an toàn HTTT

❖ Mô hình Layered Security Model hoặc Defence in Depth



1.4 Mô hình tổng quát đảm bảo an toàn HTTT

- Các lớp phòng vệ điển hình:
  - Lớp an ninh cơ quan/tổ chức (Plant Security)
    - Lớp bảo vệ vật lý
    - Lớp chính sách & thủ tục đảm bảo ATTT
  - Lớp an ninh mạng (Network Security)
    - Lớp an ninh cho từng thành phần mạng
    - Tường lửa, mạng riêng ảo (VPN)
  - Lớp an ninh hệ thống (System Security)
    - Lớp tăng cường an ninh hệ thống
    - Lớp quản trị tài khoản và phân quyền người dùng
    - Lớp quản lý các bản vá và cập nhật phần mềm
    - Lớp phát hiện và ngăn chặn phần mềm độc hại.