HỌC VIỆN HÀNG KHÔNG VIỆT NAM
**KHOA CÔNG NGHỆ THÔNG TIN**

# An toàn và bảo mật thông tin

GV: THS NGUYỄN DUY HIẾU

# Nội dung

- C1 - Tổng quan
- C2 - Phân tích đánh giá nguy cơ về ATBMTT
- C3 - Giải pháp cho ATBMTT
- C4 - Hệ thống tiêu chuẩn quản lý ATTT
- C5 - Hệ thông quản lý ATTT
- C6 - Pháp luật và chính sách ATTT

# Tài liệu học tập

| TT | Tên tác giả | Năm | Tên tài liệu | NXB |
|---|---|---|---|---|
| **I** | **Tài liệu chính** | | | |
| 1 | Michael E. Whitman and Herbert J. Mattord | 2012 | Principles of Information Security | Nelson Education |

# Phương thức đánh giá

| Điểm Quá trình | | Điểm học phần | | |
|---|---|---|---|---|
| Chuyên cần | KT TX + KT GK | Quá trình | Thi | Tổng |
| 10% | 40% | 50% | 50% | 100% |

**Hình thức đánh giá:**

- Chuyên cần: điểm danh
- Kiểm tra: Bài tập, Thực hành, trắc nghiệm.
- Thi: trắc nghiệm

Chương 1

# Tổng quan

# Nội dung

1. Khái quát về ATTT
2. Các yêu cầu đảm bảo ATTT và HTTT
3. Các thành phần của ATTT
4. Các mối đe dọa và nguy cơ ATTT trong các vùng hạ tầng CNTT
5. Mô hình tổng quát đảm bảo ATTT và HTTT

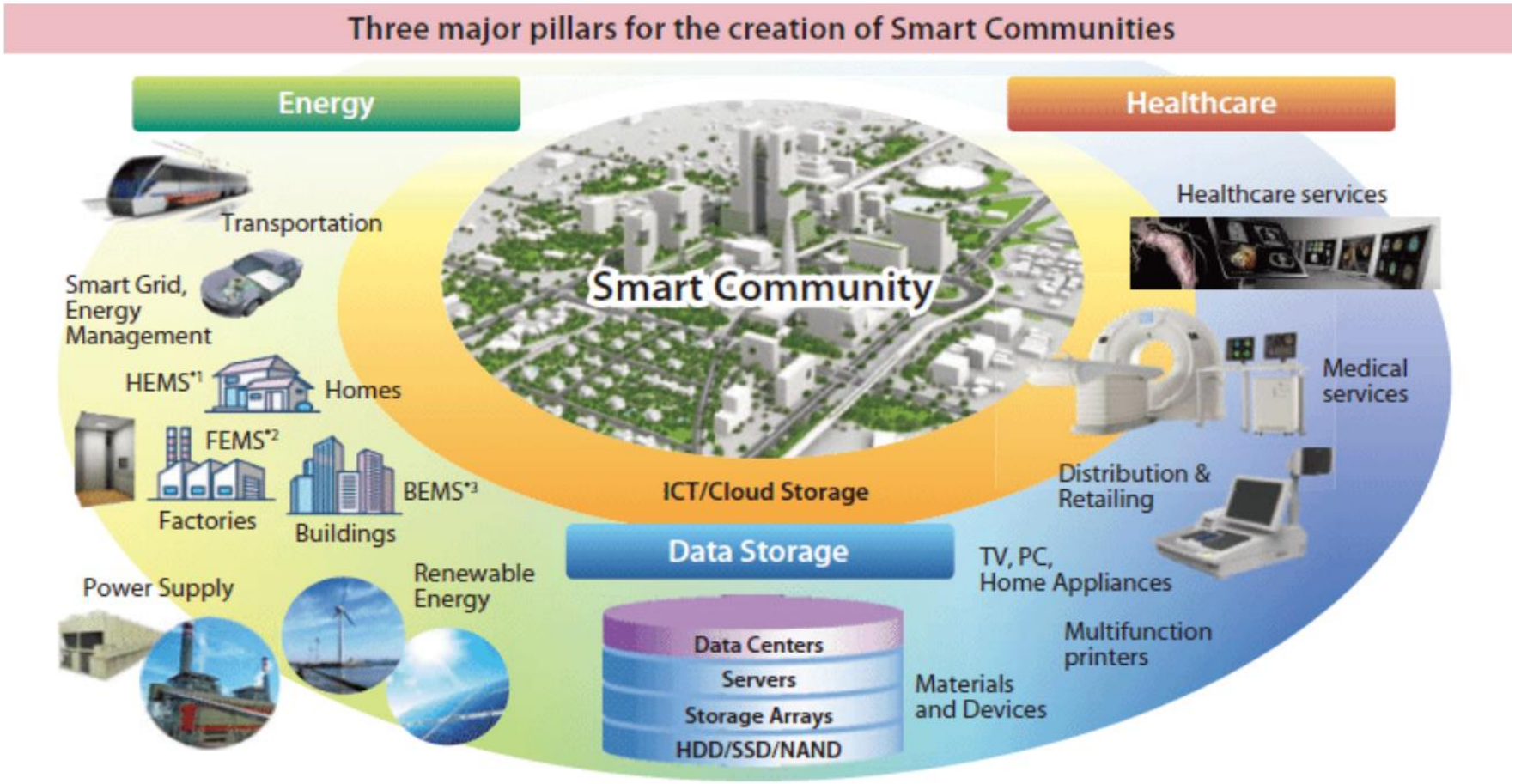
# 1. Khái quát về ATTT

- Sự cần thiết của an toàn thông tin
- Một số khái niệm trong ATTT
  - An toàn thông tin
  - Các lĩnh vực của ATTT
  - Các thành phần của ATTT
  - An toàn hệ thống thông tin
  - Mối đe dọa, điểm yếu, lỗ hổng và nguy cơ mất ATTT

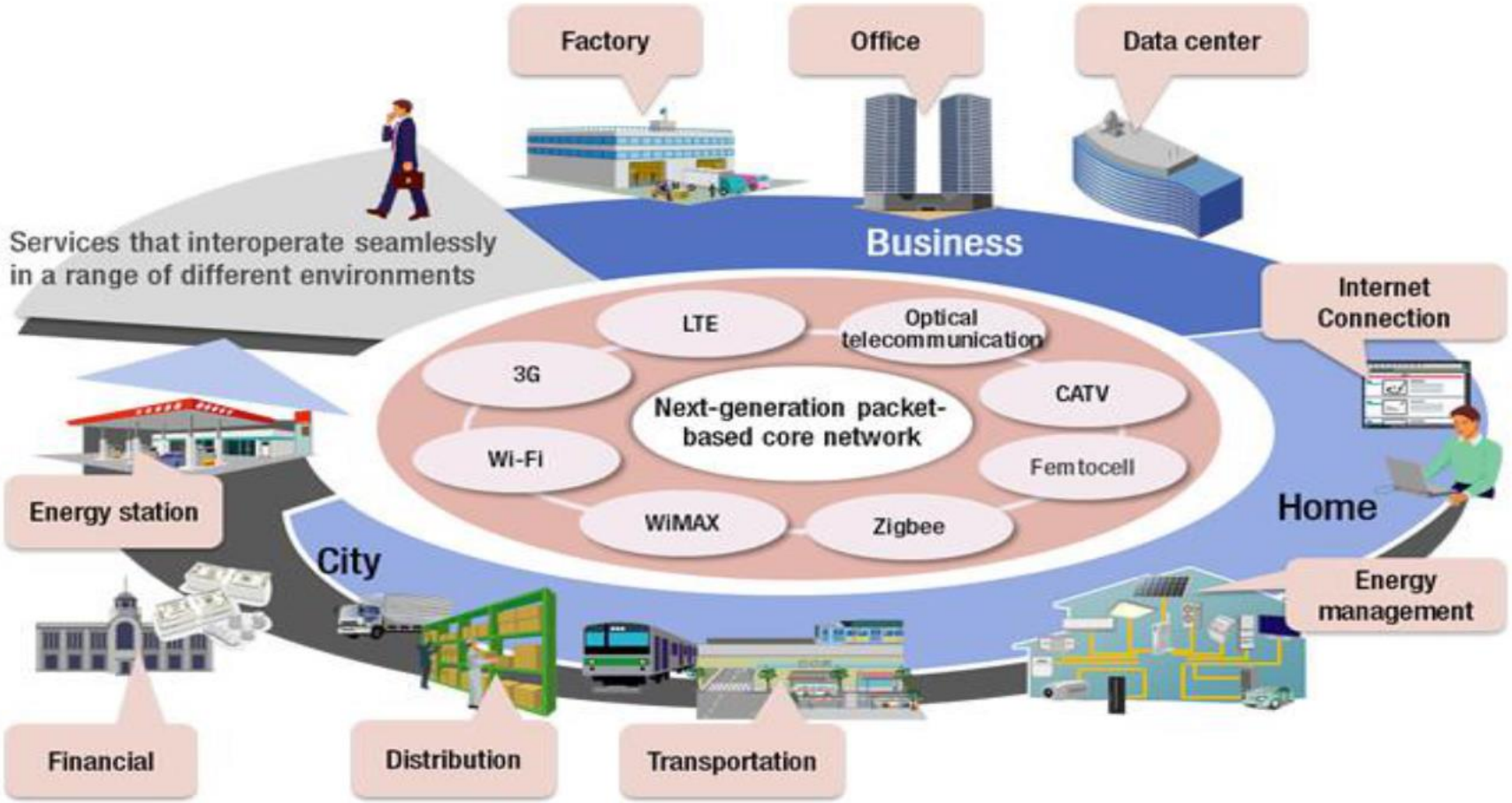
# Sự cần thiết của an toàn thông tin

- Thế giới kết nối thiết bị đa phương tiện
  - 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
    - Smart city
    - Smart home
  - Các khái niệm kết nối mọi vật, kết nối tất cả trở nên "Hot"
    - IoT: Internet of Things
    - IoE: Internet of Everything
  - Các hệ thống không có kết nối khả năng sử dụng hạn chế

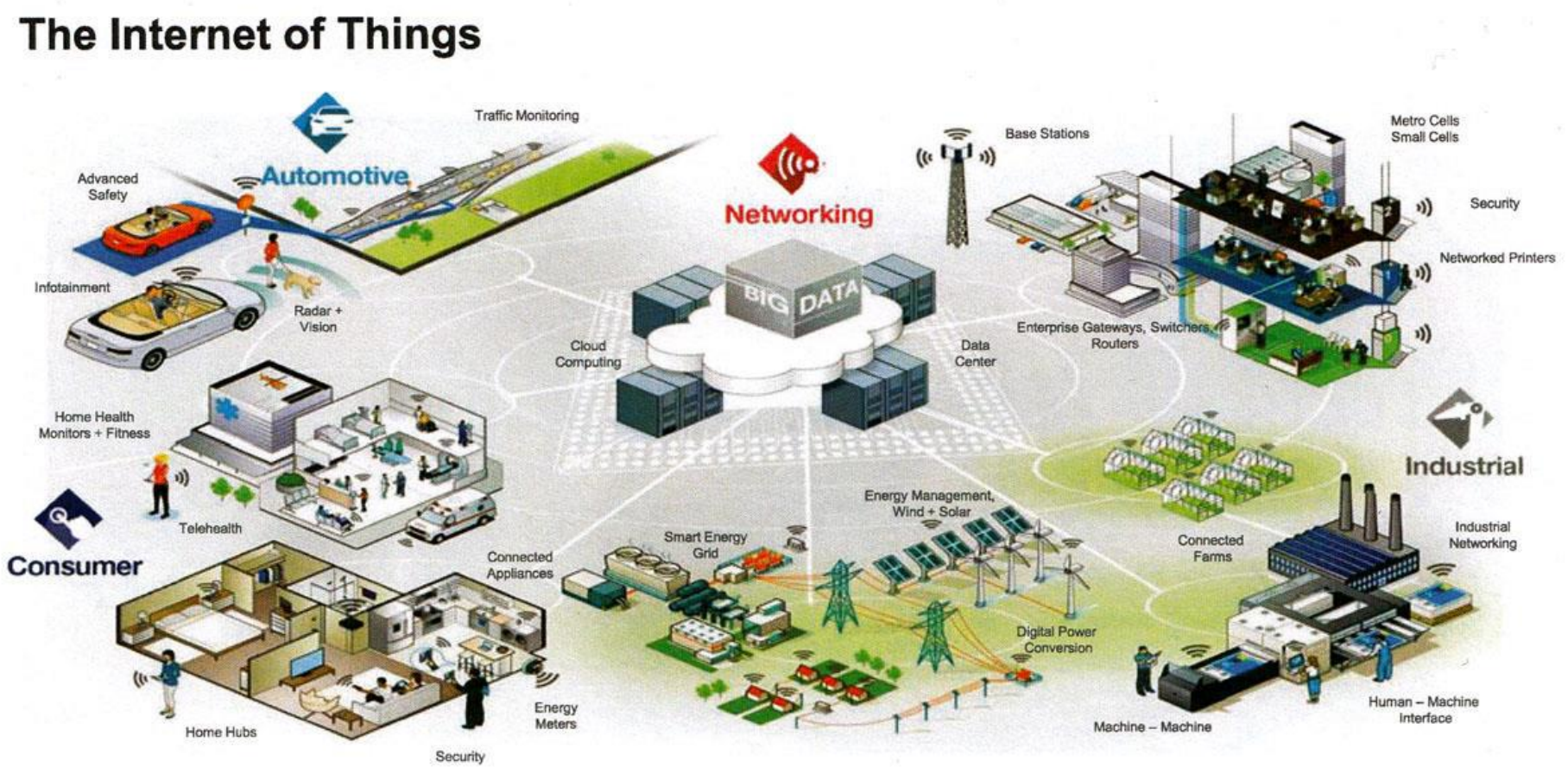
# Mô hình kết nối trong cộng đồng thông minh



# Mô hình kết nối trong Thành phố thông minh

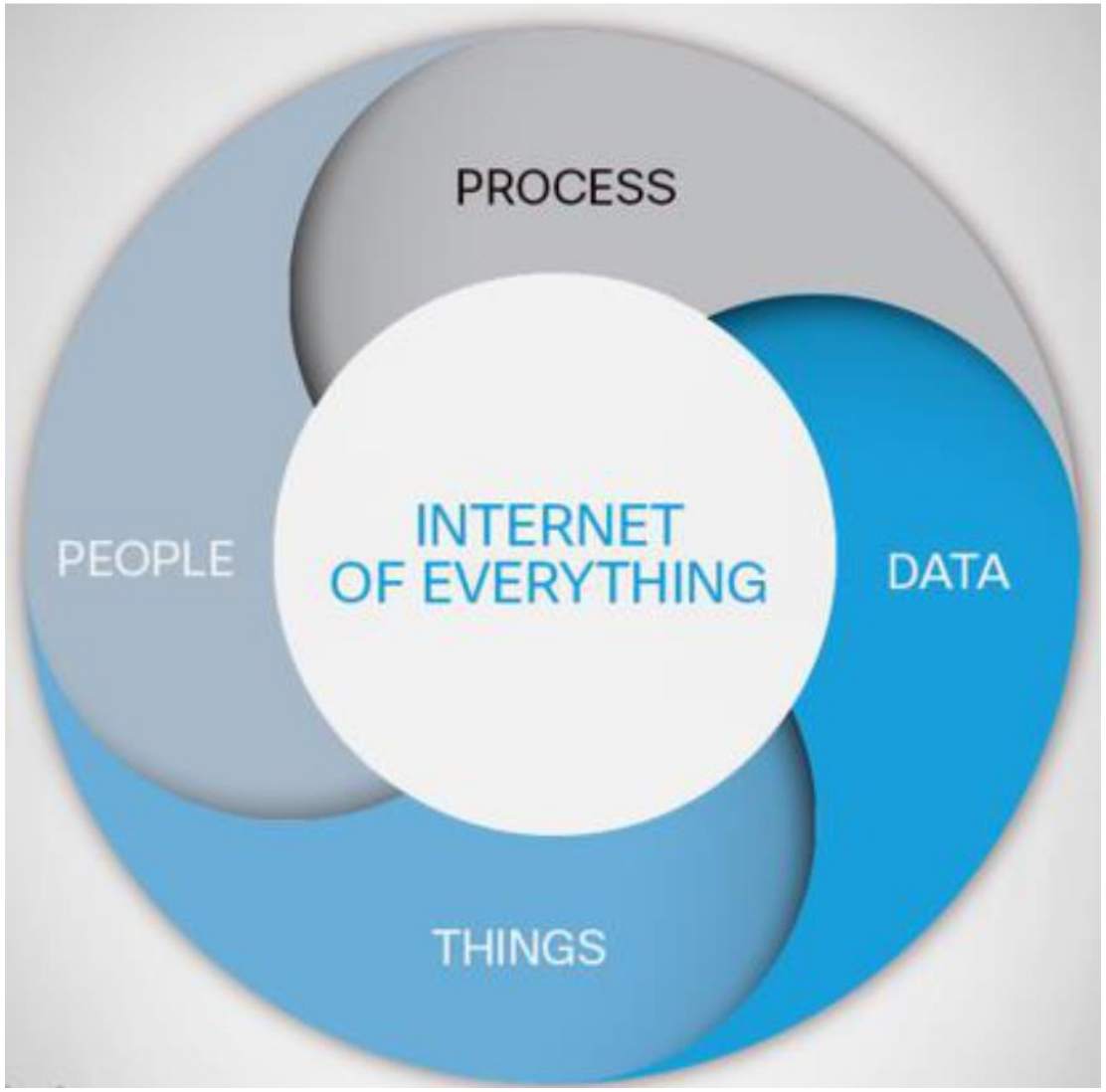


# Mô hình Internet of Things



# Mô hình Internet of Things

# Mô hình Internet of Things

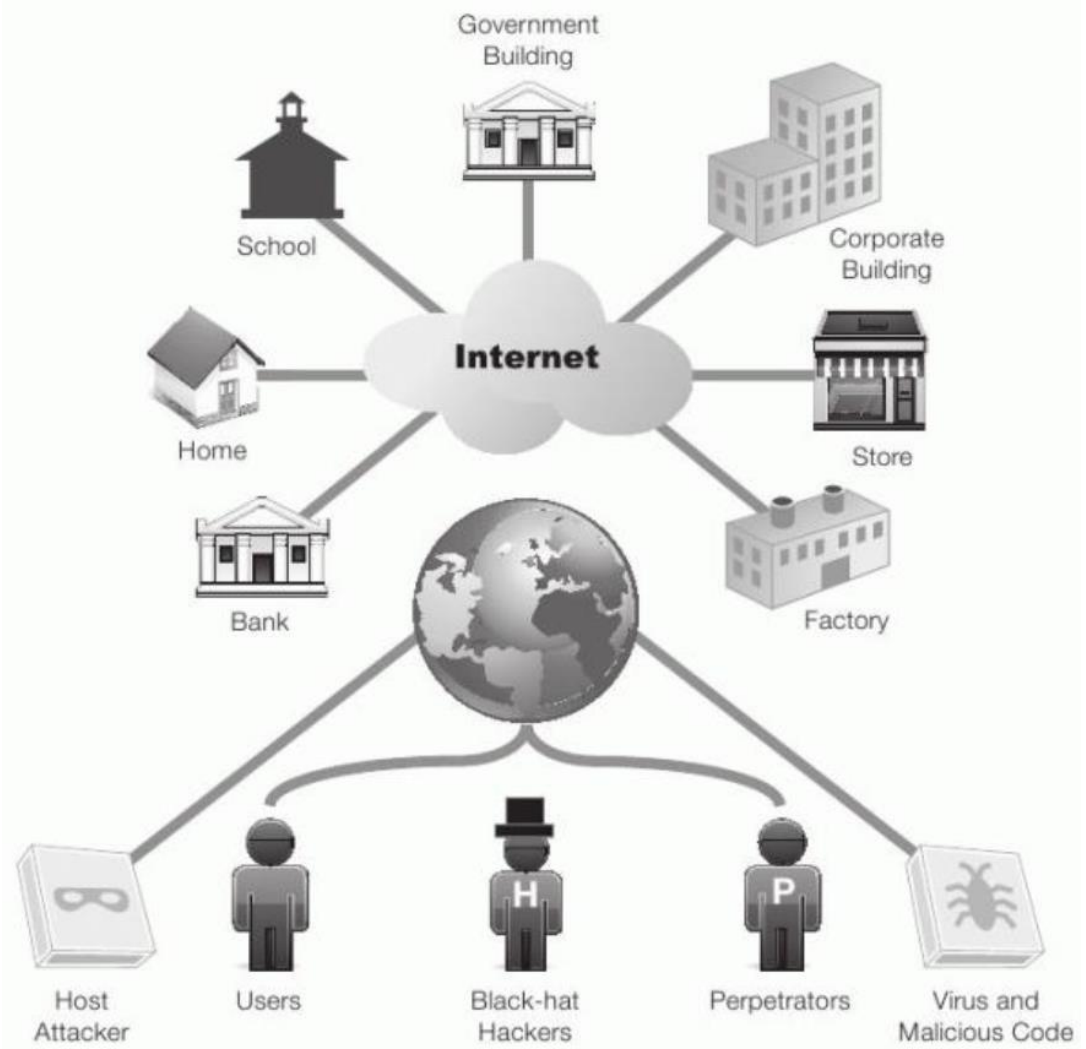


# Sự cần thiết của an toàn thông tin

- 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.

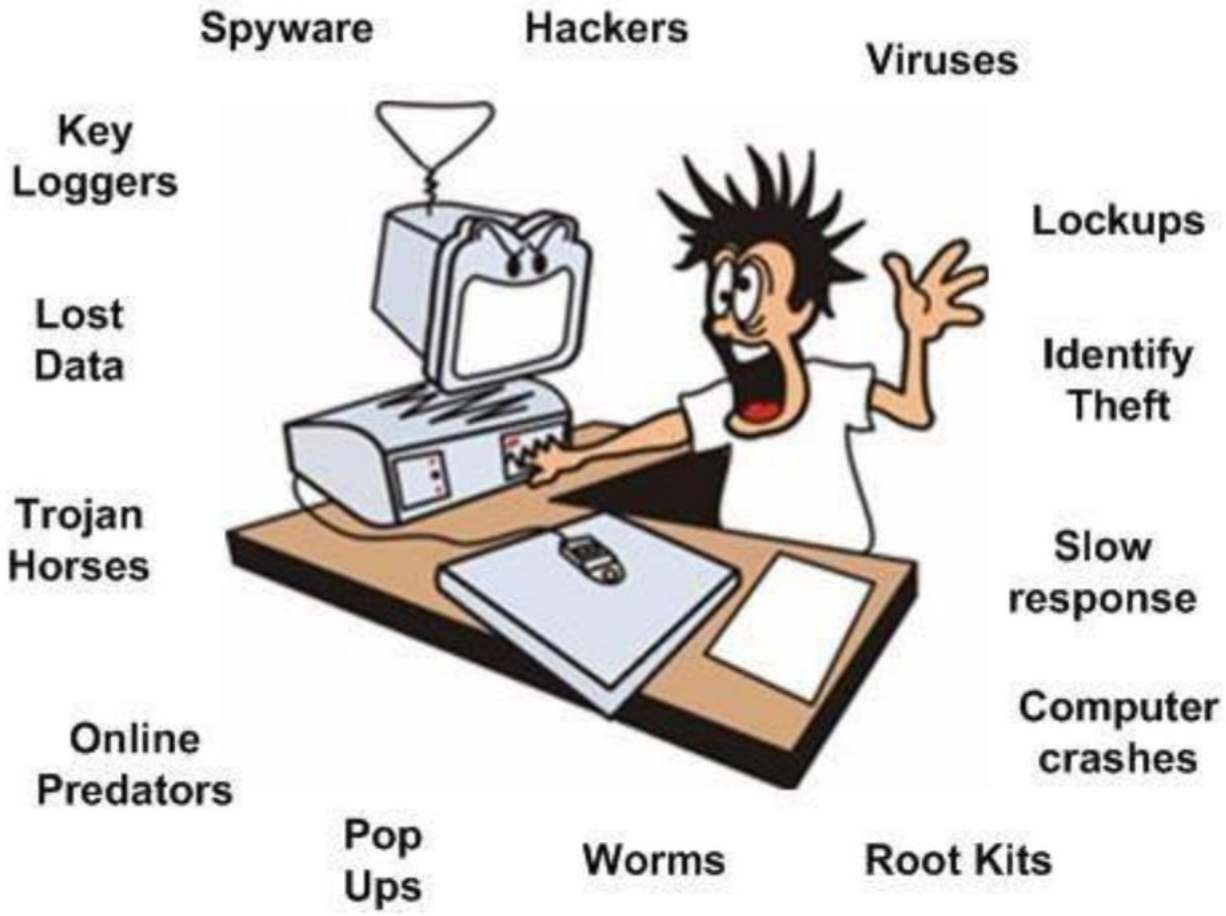
# Sự cần thiết của an toàn thông tin

Thế giới kết nối với nhiều nguy cơ và đe dọa



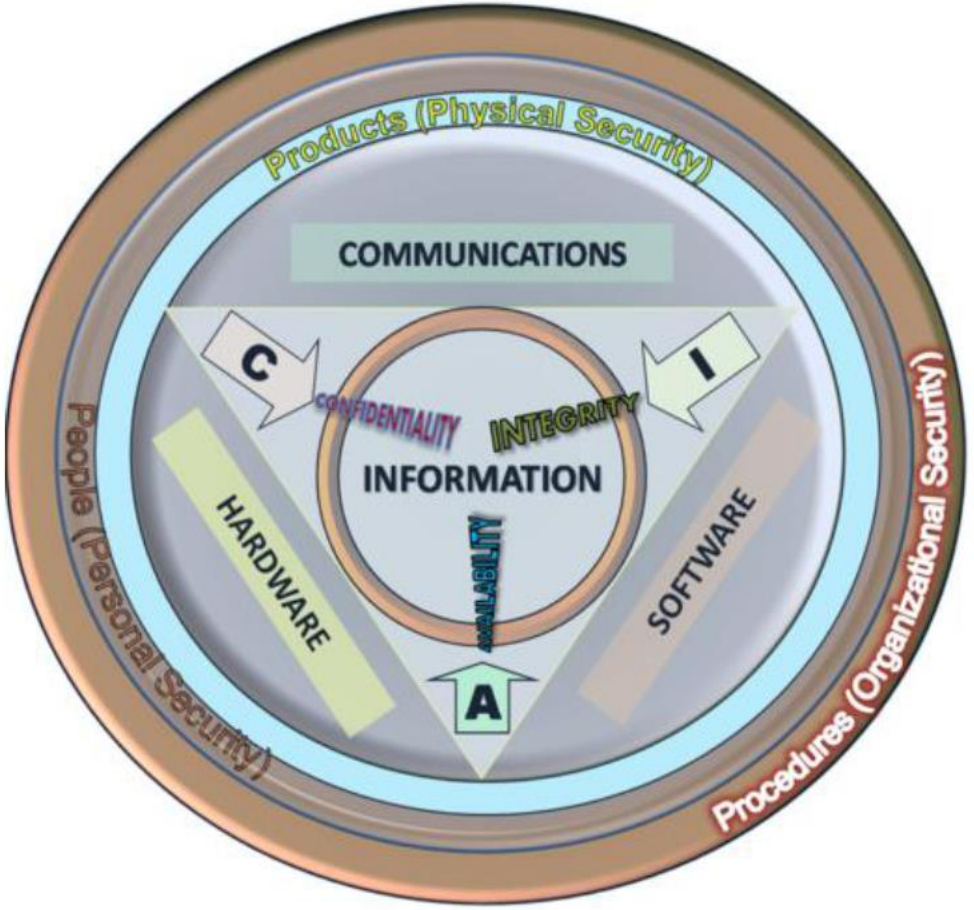
# Sự cần thiết của an toàn thông tin

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



# Một số khái niệm trong ATTT

- An toàn thông tin 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.
  - An toàn thông tin còn bao gồm cả việc đảm bảo an toàn cho các thành phần, hoặc hệ thống được sử dụng để quản lý, lưu trữ, xử lý và trao đổi thông tin.



# Một số khái niệm trong ATTT

- Các lĩnh vực chính của an toàn thông tin
  - 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 thông tin
    - 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).

# Một số khái niệm trong ATTT

- 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)

# Một số khái niệm trong ATTT

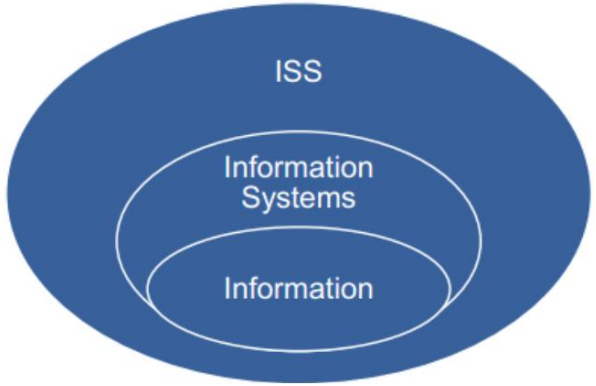
- Hệ thống thông tin
  - Hệ thống tích hợp các thành phần phục vụ:
    - Thu thập, lưu trữ, xử lý thông tin
    - Chuyển giao thông tin, tri thức và các sản phẩm số.
  - Các doanh nghiệp và các tổ chức sử dụng các hệ thống thông tin (HTTT) để thực hiện và quản lý các hoạt động
    - Tương tác với khác 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.

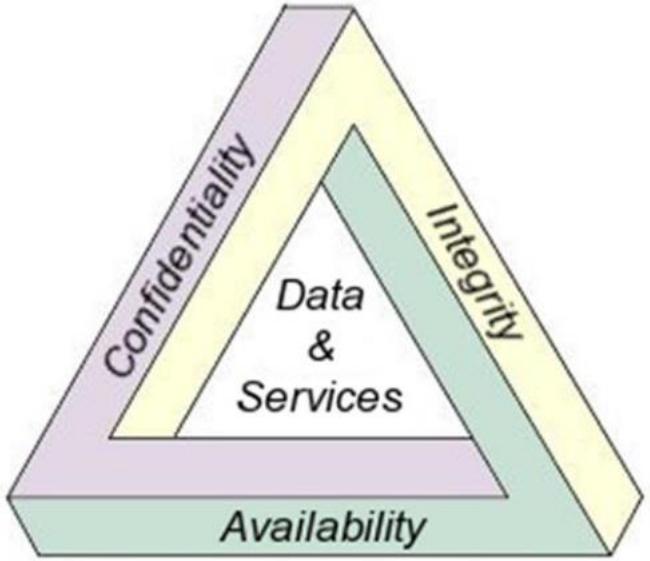
# Một số khái niệm trong ATTT

- 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.

# Một số khái niệm trong ATTT

- 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)



# Một số khái niệm trong ATTT

- Mối đe dọa (threat): Mối đe dọa là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống (gồm phần cứng, phần mềm, CSDL, các file, dữ liệu, hoặc hạ tầng mạng vật lý,…).
- Điểm yếu (weakness): là những khiếm khuyết hoặc lỗi tồn tại trọng hệ thống:
  - Điểm yếu phần cứng
  - Điểm yếu phần mềm (Hệ điều hành và ứng dụng)
- Lỗ hổng (vulnerability): là bất kỳ điểm yếu nào trong hệ thống cho phép mối đe dọa có thể gây tác hại.

# Một số khái niệm trong ATTT

- Nguy cơ (risk): là tiềm năng một mối đe dọa có thể khai khác một lỗ hổng để tấn công hoặc gây nguy hiểm cho hệ thống.
  - Nguy cơ xuất hiện khi có mối đe dọa và lỗ hổng bảo mật.
  - Nếu tồn tại một lỗ hổng trong hệ thống, sẽ có khả năng một mối đe dọa trở thành hiện thực
  - Không thể triệt tiêu được hết các mối đe dọa, nhưng có thể giảm thiểu các lỗ hổng, qua đó giảm thiểu khả năng bị tận dụng để tấn công.

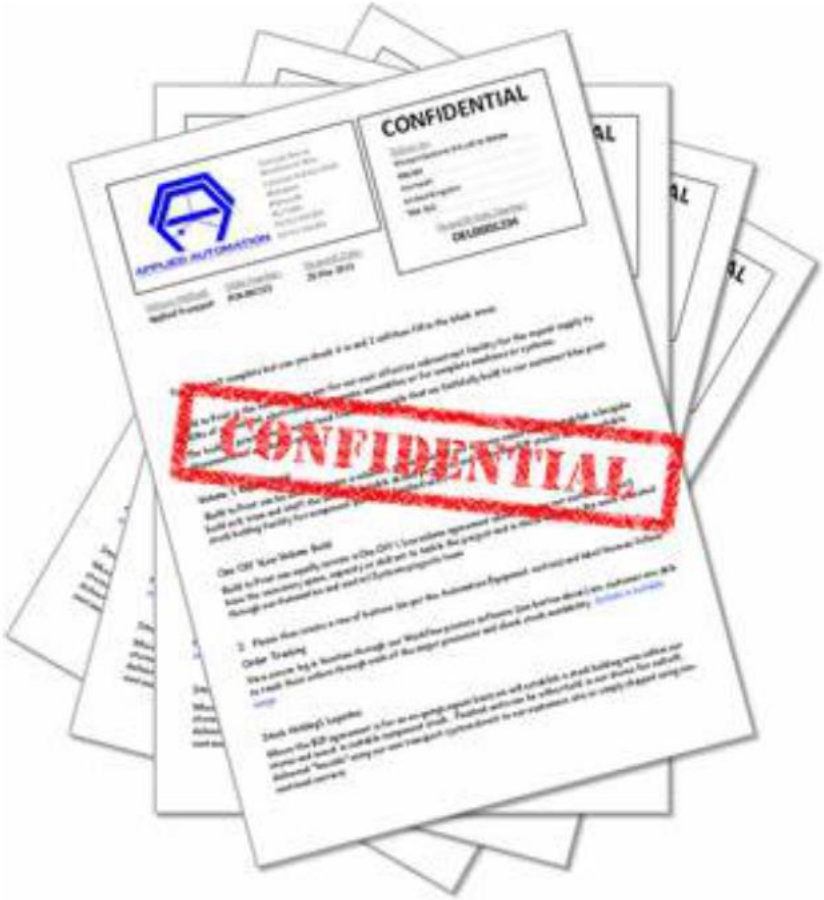
# 2. Các yêu cầu đảm bảo ATTT và HTTT

- Bí mật (Confidentiality)
- Toàn vẹn (Integrity)
- Sẵn dùng/khả dụng (Availability)

# 2. Các yêu cầu đảm bảo ATTT và HTTT

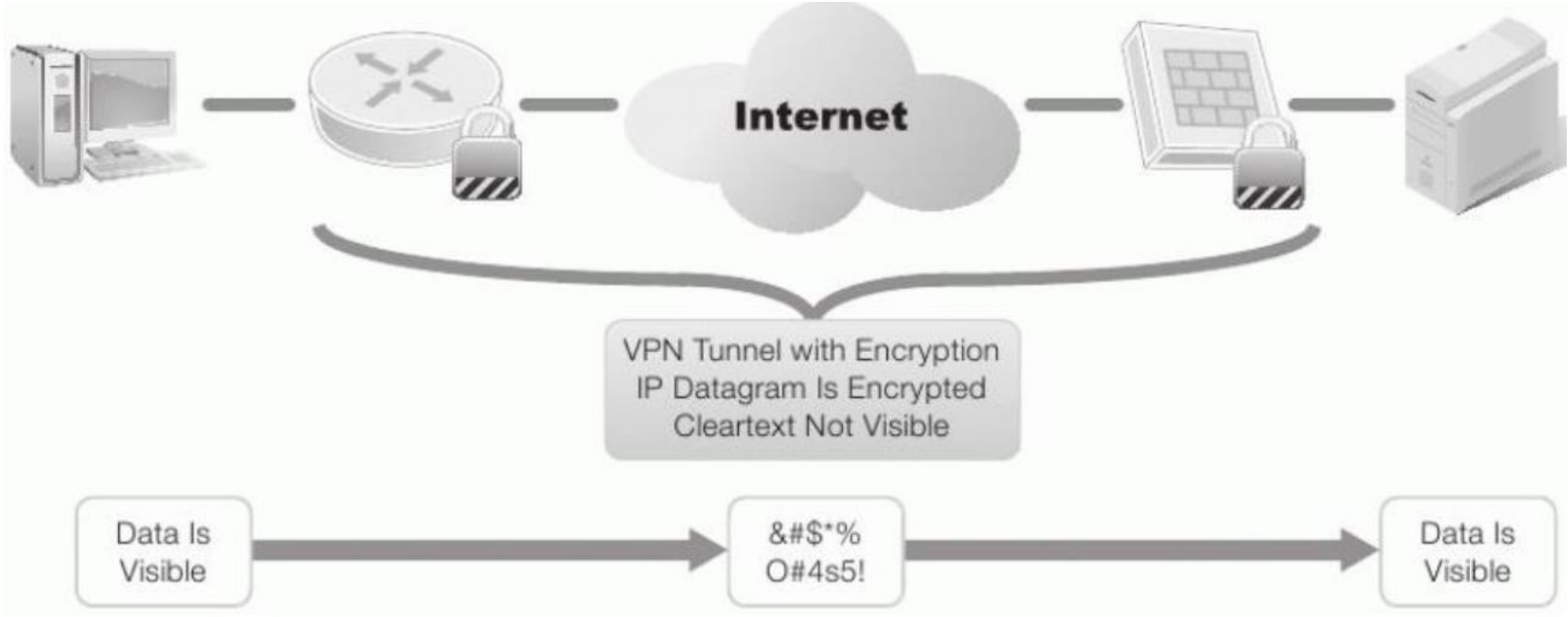
## *Tính Bí mật (Confidentiality)*

- 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.



# 2. Các yêu cầu đảm bảo ATTT và HTTT

- Tính bí mật có thể được đảm bảo bằng kênh mã hóa VPN



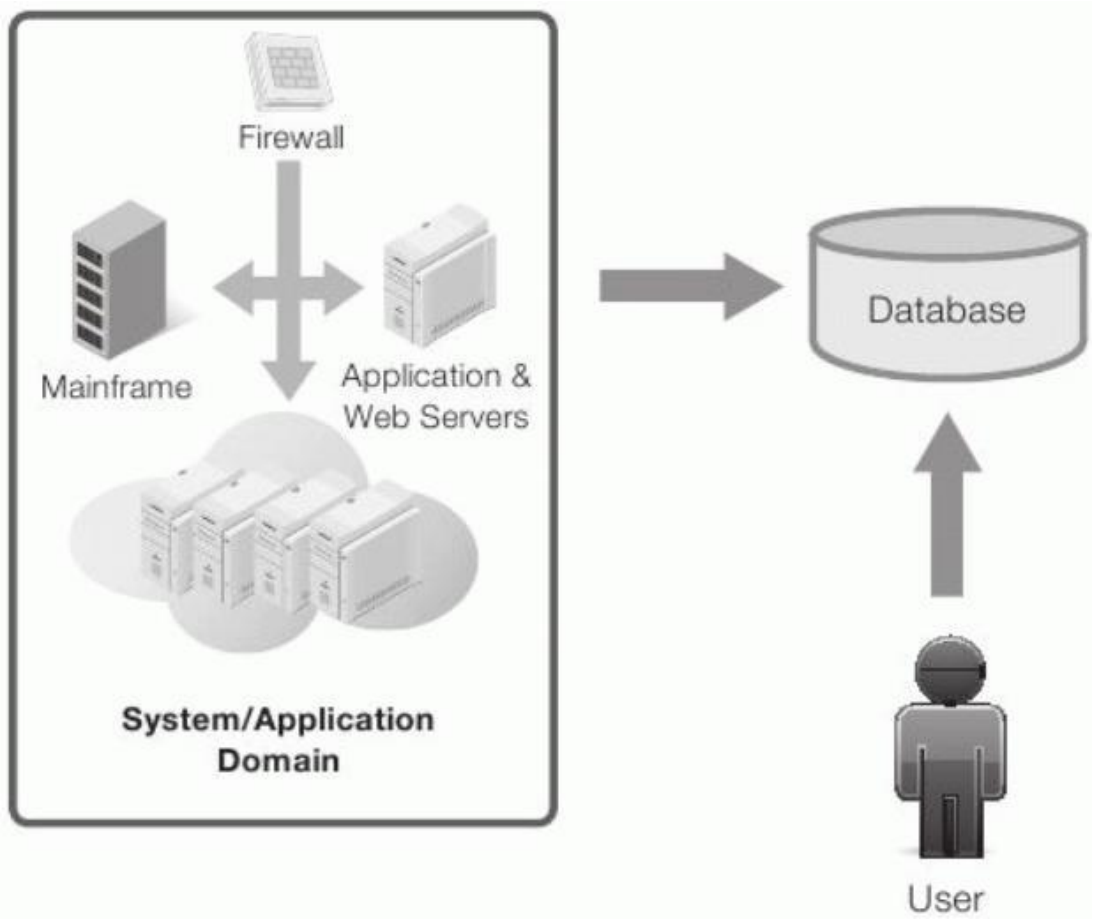
# 2. Các yêu cầu đảm bảo ATTT và HTTT

***Tính toàn vẹn (Integrity):***

- Thông tin chỉ được sửa đổi bởi những người dùng có thẩm quyền
- Liên quan đến tính hợp lệ (validity) và chính xác (accuracy) của DL
  - Thông tin có giá trị: 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.

# 2. Các yêu cầu đảm bảo ATTT và HTTT

- Tính toàn vẹn: CSDL chỉ có thể được truy nhập hay sửa đổi bởi người dùng có thẩm quyền.

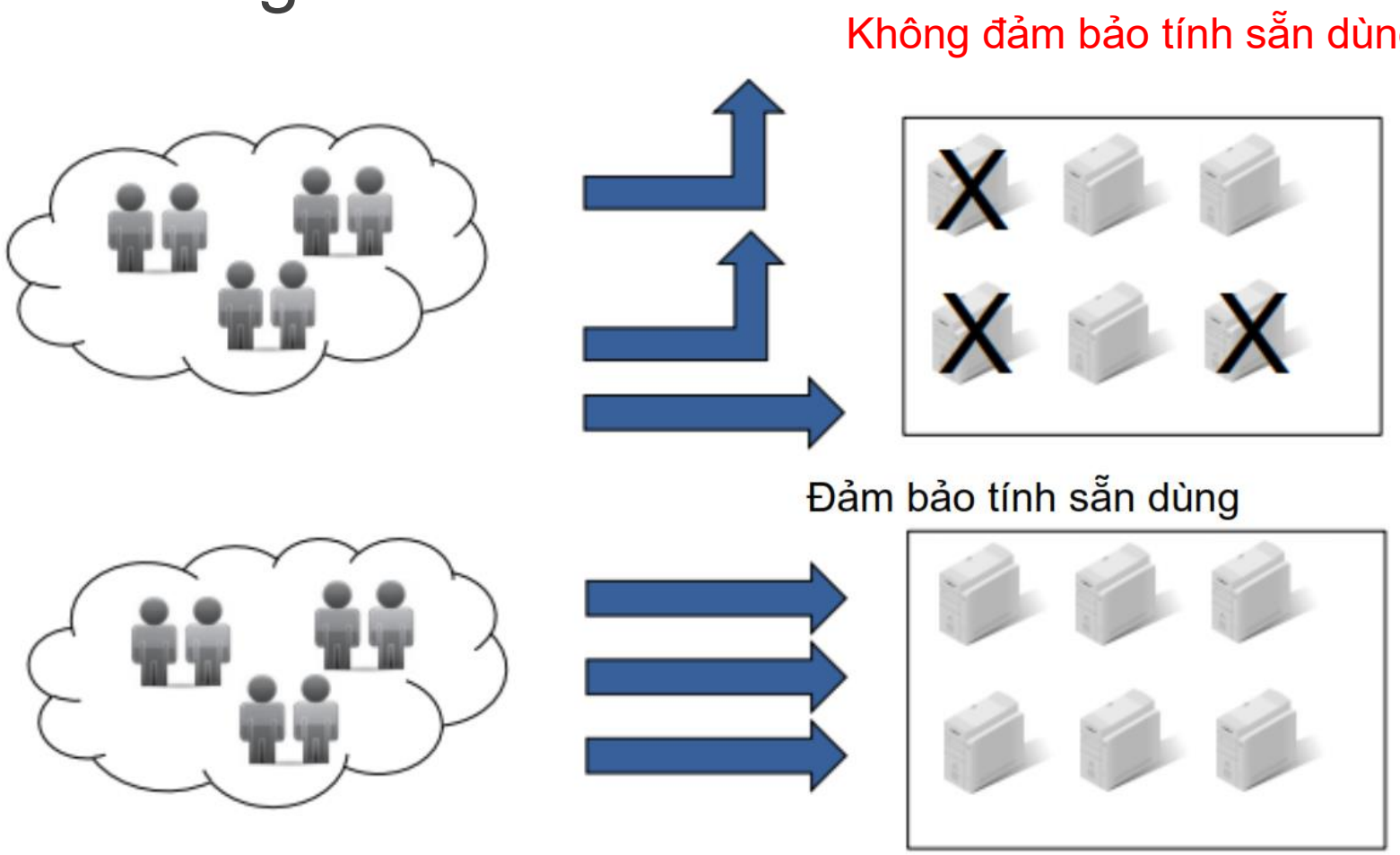


# 2. Các yêu cầu đảm bảo ATTT và HTTT

- 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.

# 2. Các yêu cầu đảm bảo ATTT và HTTT

- Tính sẵn dùng



# 3. 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)

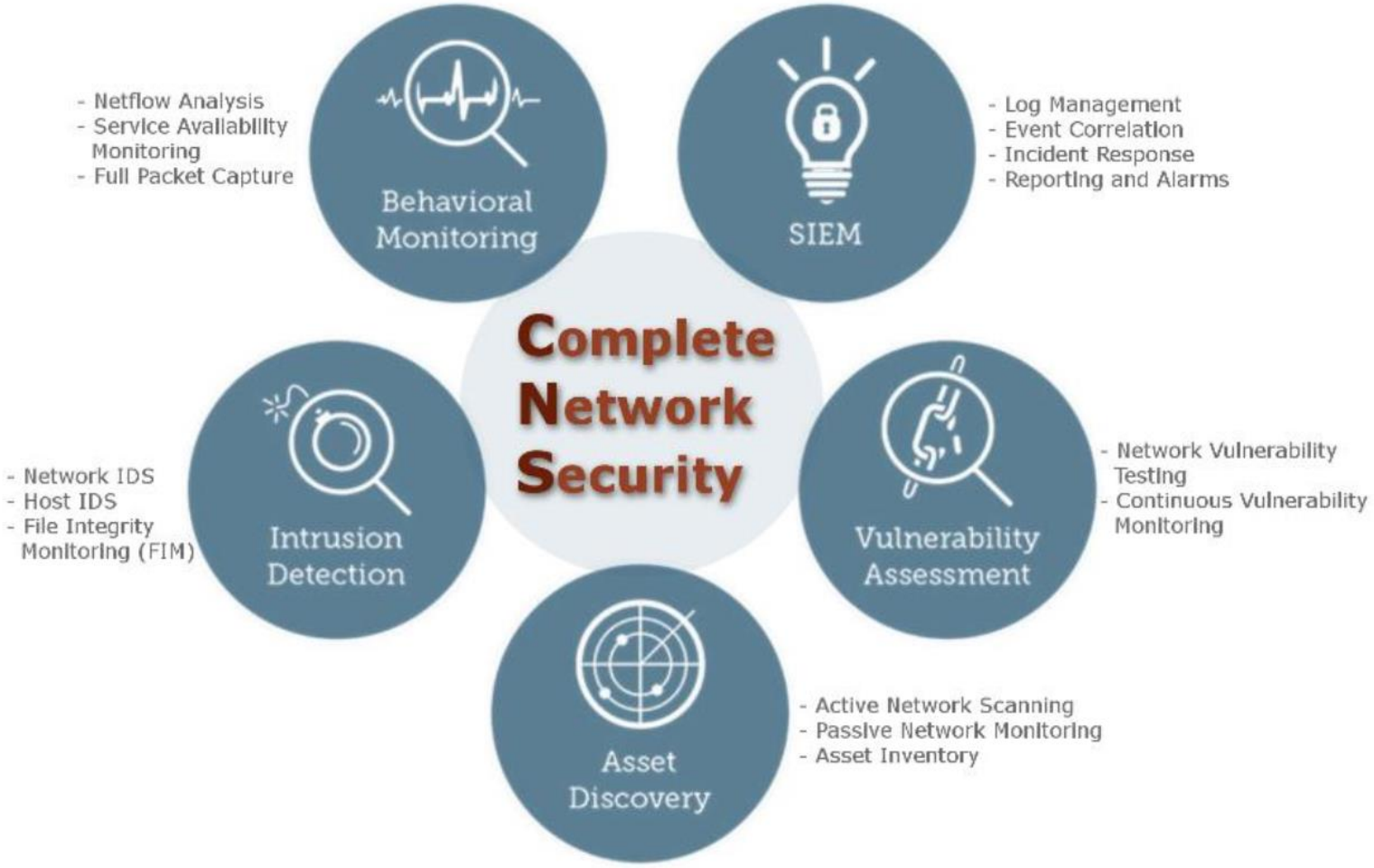
# An toàn máy tính và dữ liệu

- An toàn hệ điều hành
- An toàn ứng dụng/dịch vụ
- Điều khiển truy cập
- Mã hóa/bảo mật dữ liệu
- Phòng chống phần mềm độc hại
- Sao lưu tạo dự phòng dữ liệu

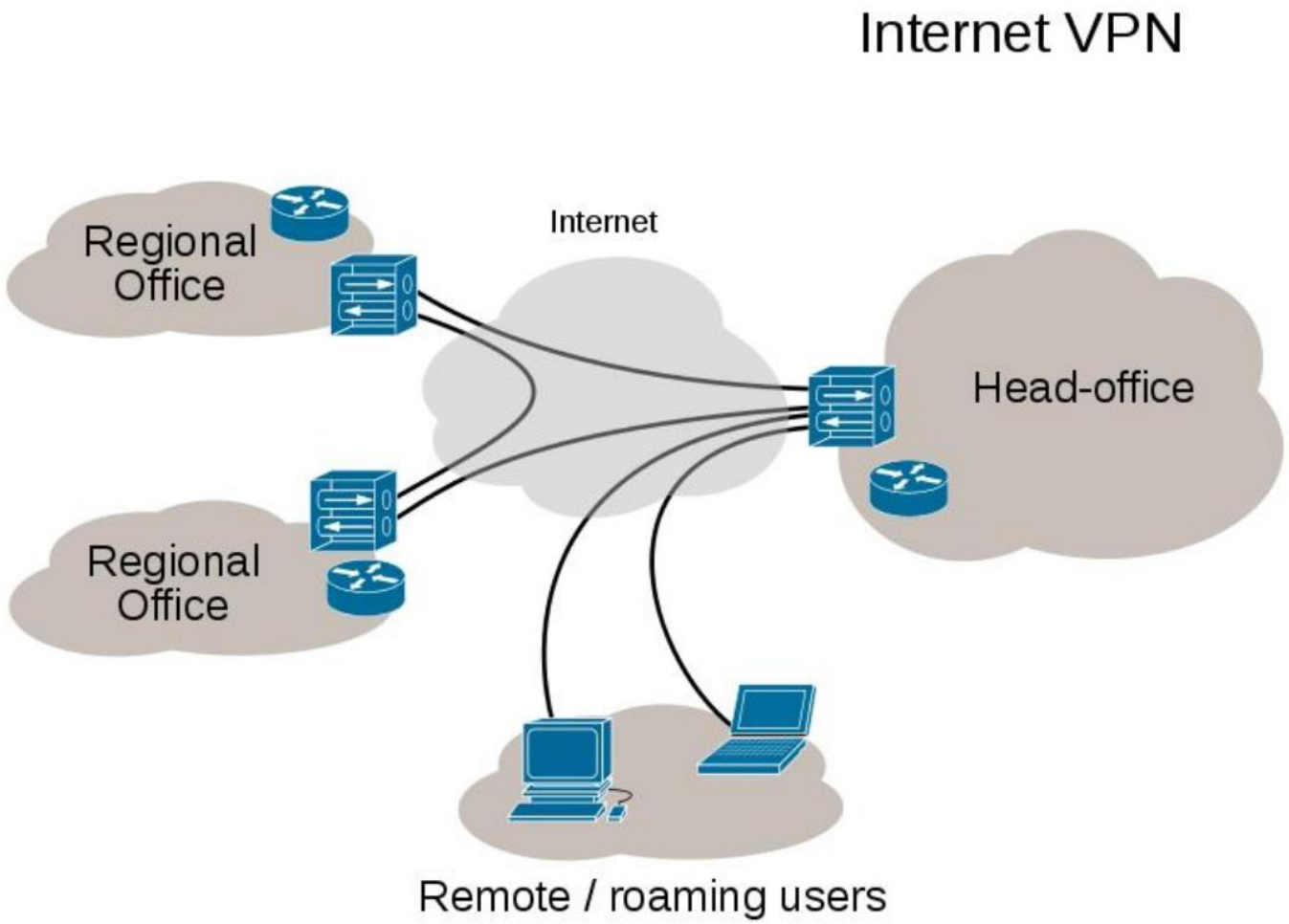
# An ninh mạng

- Tưởng lửa (Firewall)
- Mạng riêng ảo (VPN)
- Bảo mật dữ liệu truyền
- Phát hiện/ngăn chặn tấn công, xâm nhập (IPS/IDS)
- Giám sát mạng

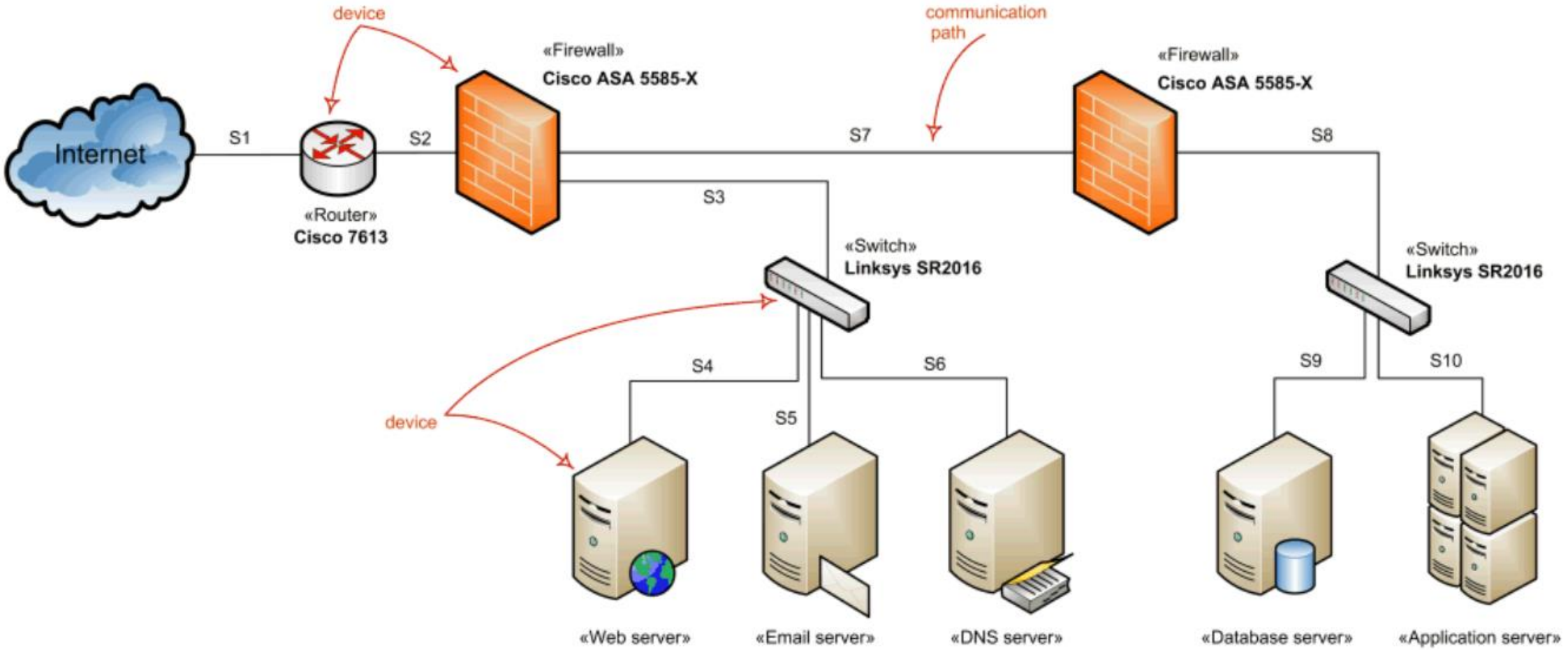
# An ninh mạng


- Netflow Analysis
- Service Availability Monitoring
- Full Packet Capture
Behavioral Monitoring
SIEM
- Log Management
- Event Correlation
- Incident Response
- Reporting and Alarms
Complete Network Security
- Network IDS
- Host IDS
- File Integrity Monitoring (FIM)
Intrusion Detection
Vulnerability Assessment
- Network Vulnerability Testing
- Continuous Vulnerability Monitoring
Asset Discovery
- Active Network Scanning
- Passive Network Monitoring
- Asset Inventory

# An ninh mạng


Internet VPN
Internet
Regional Office
Regional Office
Head-office
Remote / roaming users

# An ninh mạng


device
communication path
«Firewall»
Cisco ASA 5585-X
«Firewall»
Cisco ASA 5585-X
Internet
S1
S2
S7
S8
«Router»
Cisco 7613
S3
«Switch»
Linksys SR2016
«Switch»
Linksys SR2016
S4
S6
S9
S10
device
S5
«Web server»
«Email server»
«DNS server»
«Database server»
«Application server»

# Quản lý an toàn thông tin

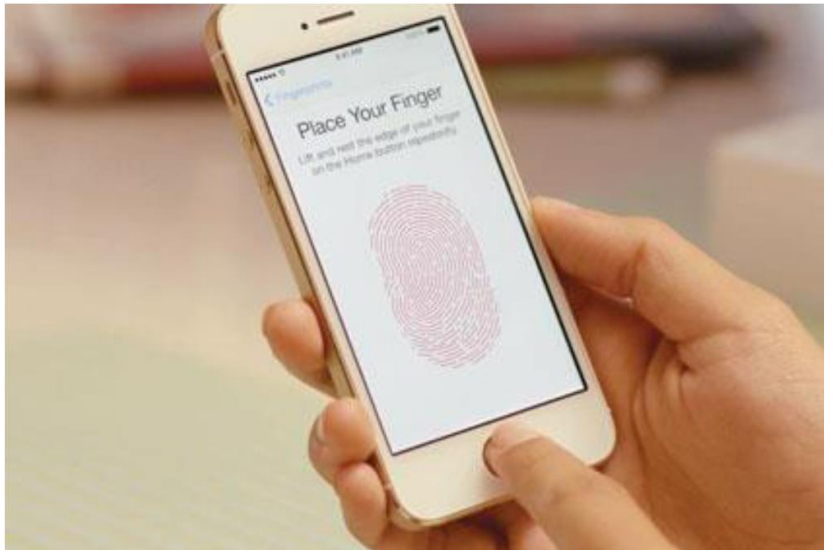
- Quản lý rủi ro (risk)
- Các chuẩn ATTT
- Chính sách ATTT
- Đào tạo người dùng

# Chính sách an toàn thông tin

- Chính sách ATTT ở mức vật lý (Physical security policy)
- Chính sách ATTT ở mức tổ chức (Orgranisational security policy)
- Chính sách ATTT ở mức logic (Logical security policy)

# Chính sách an toàn thông tin

- Áp dụng chính sách xác thực ‘mạnh’ sử dụng đặc đặc điểm sinh trắc (Biometric) thay cho mật khẩu truyền thống

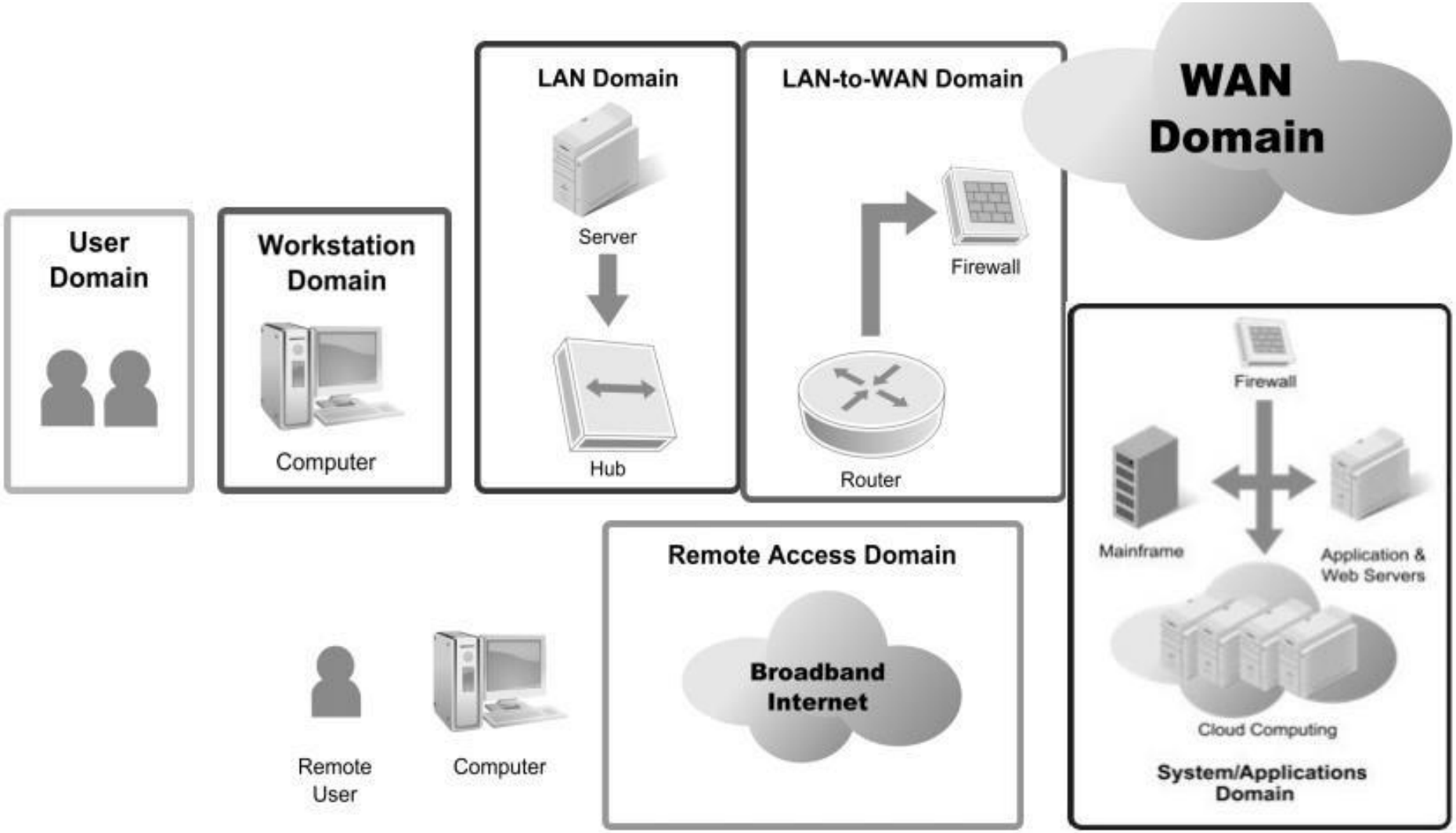
# Các mối đe dọa và nguồn nguy cơ với HTTT

- Bảy vùng trong cơ sở hạ tầng CNTT
- Các mối đe dọa và nguy cơ trong các vùng hạ tầng CNTT

# Bảy vùng trong cơ sở hạ tầng CNTT

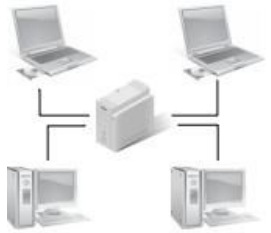
- Vùng người dùng (User domain)
- Vùng máy trạm (Workstation domain)
- Vùng mạng LAN (LAN domain)
- Vùng LAN-to-WAN (LAN-to-WAN domain)
- Vùng WAN (WAN domain)
- Vùng truy nhập từ xa (Remote Access domain)
- Vùng hệ thống/ứng dụng (Systems/Applications domain)

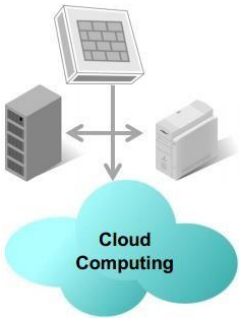
# Bảy vùng trong cơ sở hạ tầng CNTT



# Các mối đe dọa và nguồn nguy cơ với HTTT

- Các đe dọa/nguy cơ với người dùng
- Các đe dọa/nguy cơ với vùng máy trạm
- Các đe dọa/nguy cơ với vùng LAN
- Các đe dọa/nguy cơ với vùng LAN-to-WAN
- Các đe dọa/nguy cơ với vùng WAN
- Các đe dọa/nguy cơ với vùng truy nhập từ xa
- Các đe dọa/nguy cơ với vùng hệ thống/ứng dụng



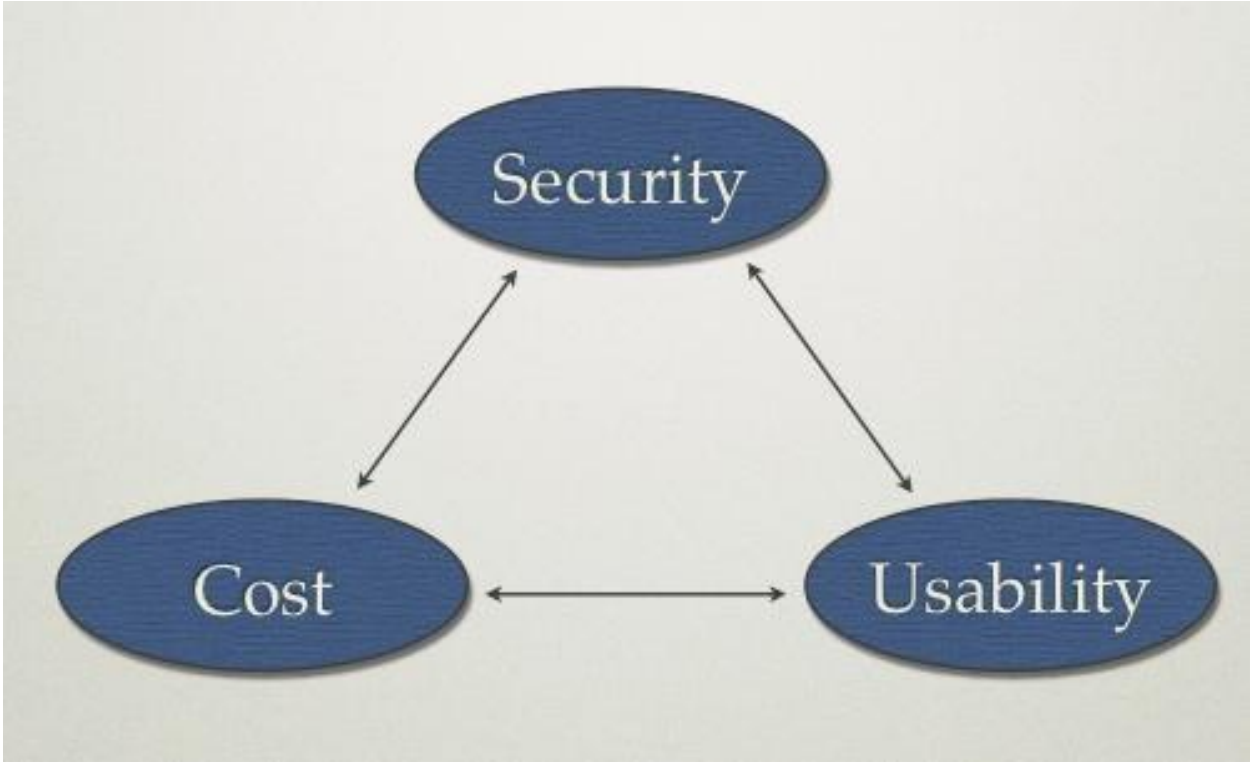


# Quy trình quản lý các nguy cơ

- 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 riêng rẽ 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 vấn đề an toàn, tính hữu dụng và chi phí đầu tư.

# Quy trình quản lý các nguy cơ

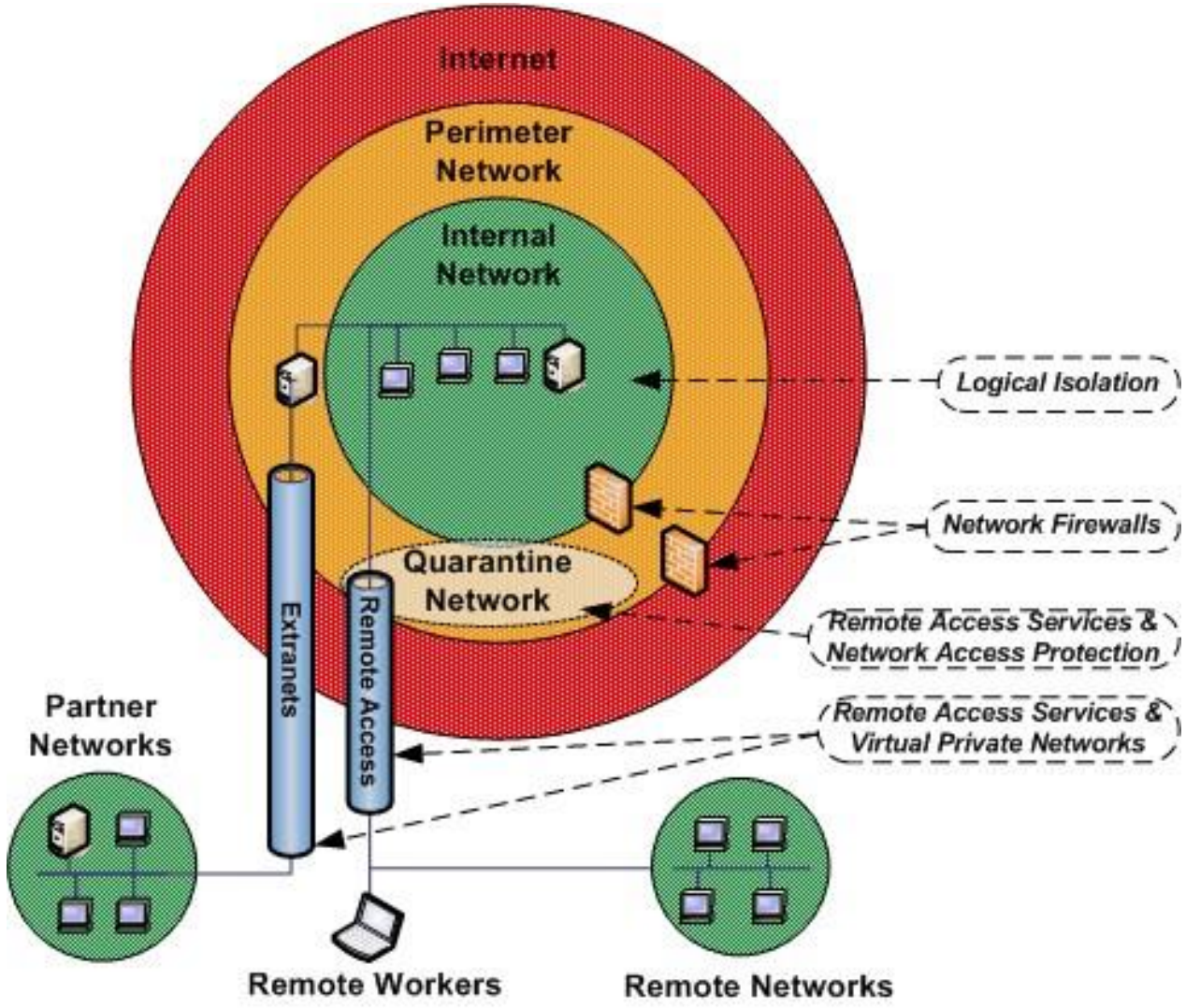
- Cần cân bằng giữa Usability (Tính hữu dụng), Cost (chi phí) và Security (an toàn)



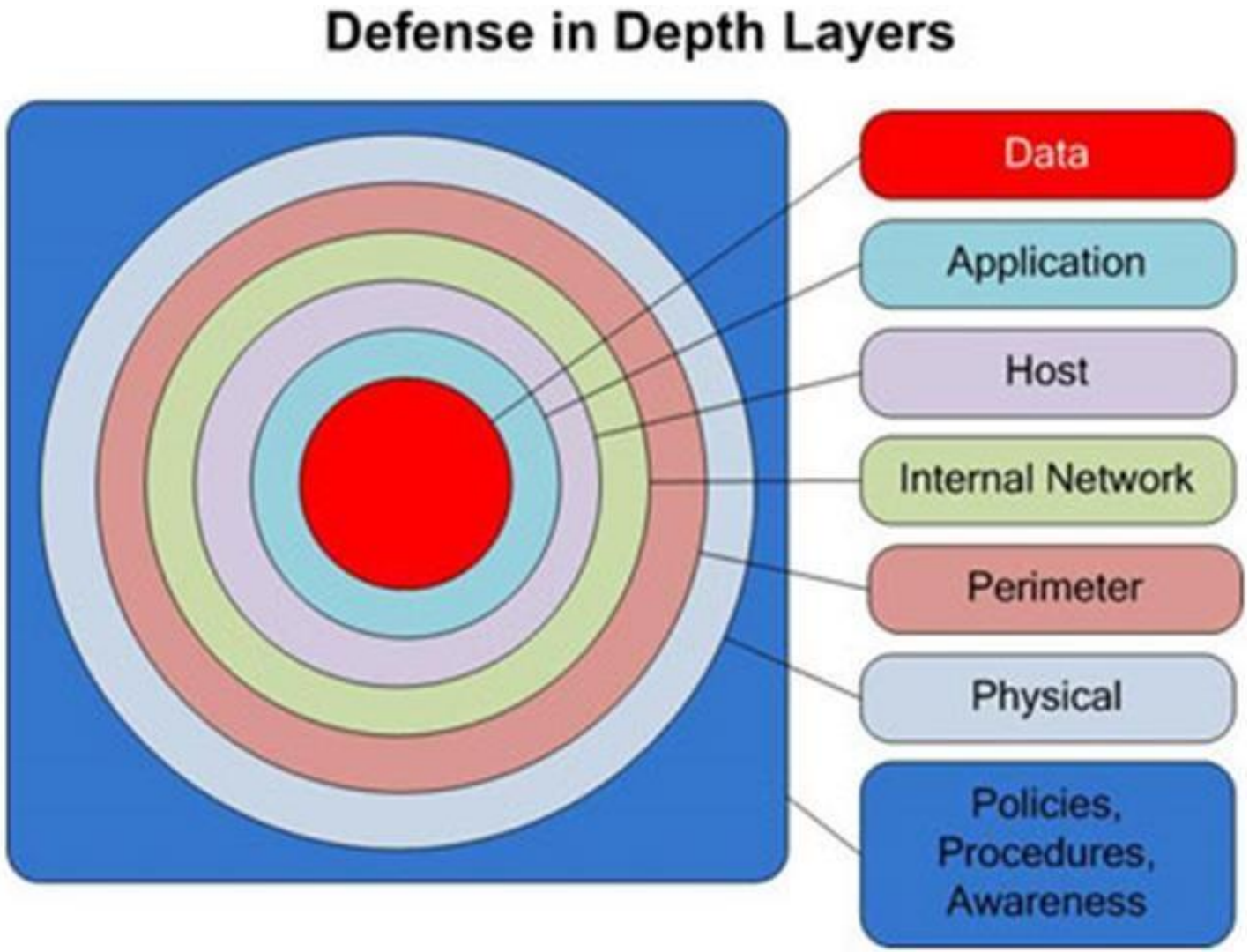
# Giải pháp đảm bảo AT & BMTT

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

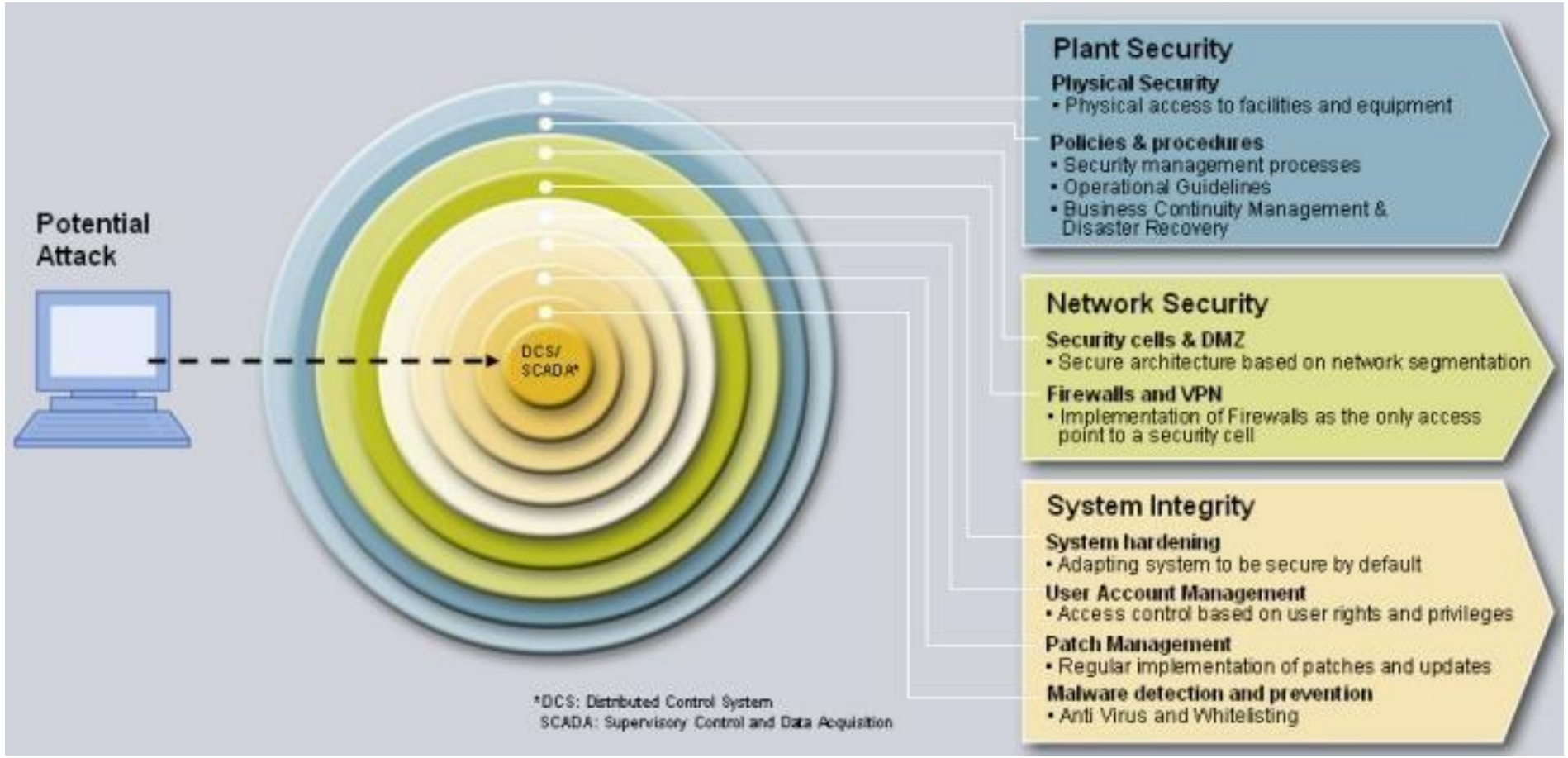
# Một số mô hình tổng quát đảm bảo ATTT và HTTT



# Một số mô hình tổng quát đảm bảo ATTT và HTTT



# Một số mô hình tổng quát đảm bảo ATTT và HTTT



# Một số mô hình tổng quát đảm bảo ATTT và HTTT

***Các lớp phòng vệ điển hình trong mô hình phòng vệ nhiều lớp***

- 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.

# Kết thúc