AN TOÀN THÔNG TIN

information security

Chương I.

Tổng quan về An toàn thông tin

1. Dẫn nhập (introduction)
2. Lịch sử (History)
3. Định nghĩa bảo mật
4. Các thành phần HTTT
5. Tiếp cận phương pháp bảo mật thông tin

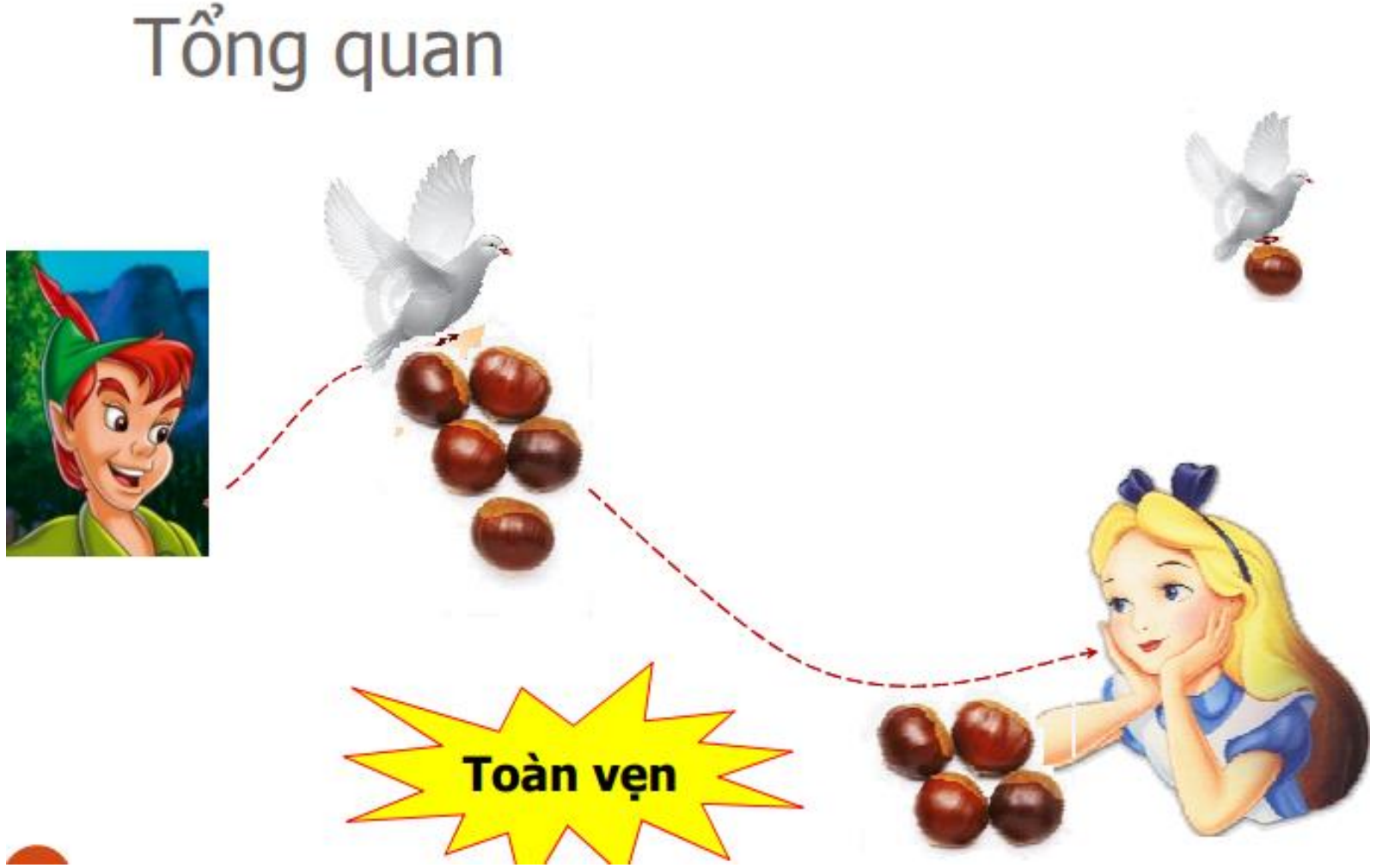
1. Dẫn nhập tình huống 1

Tổng quan

Mình đã biết hết những gì bọn chúng trao đổi với nhau.

Bí mật

1. Dẫn nhập tình huống 2

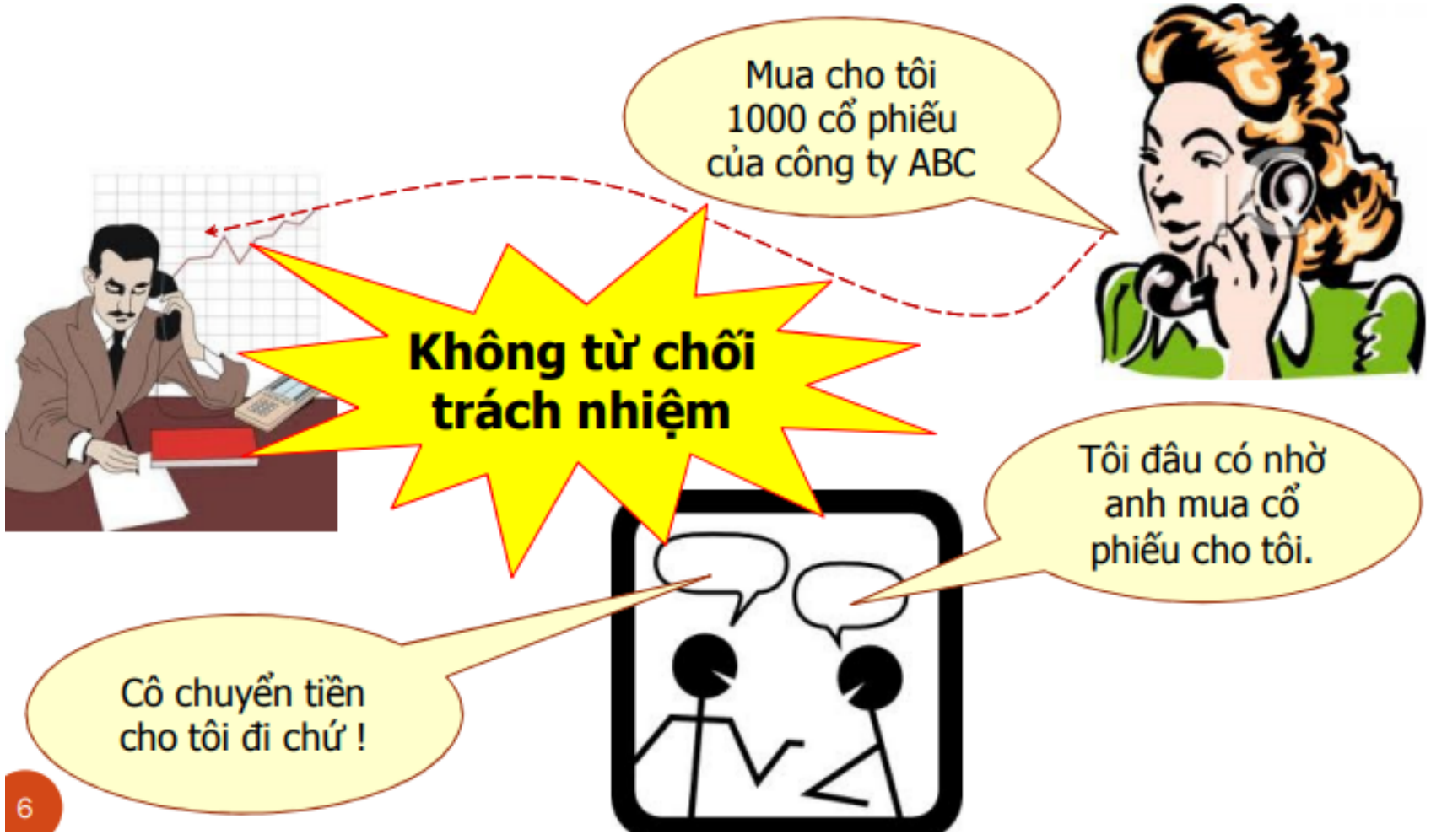


1. Dẫn nhập tình huống 3

Tổng quan

1. Dẫn nhập tình huống 4

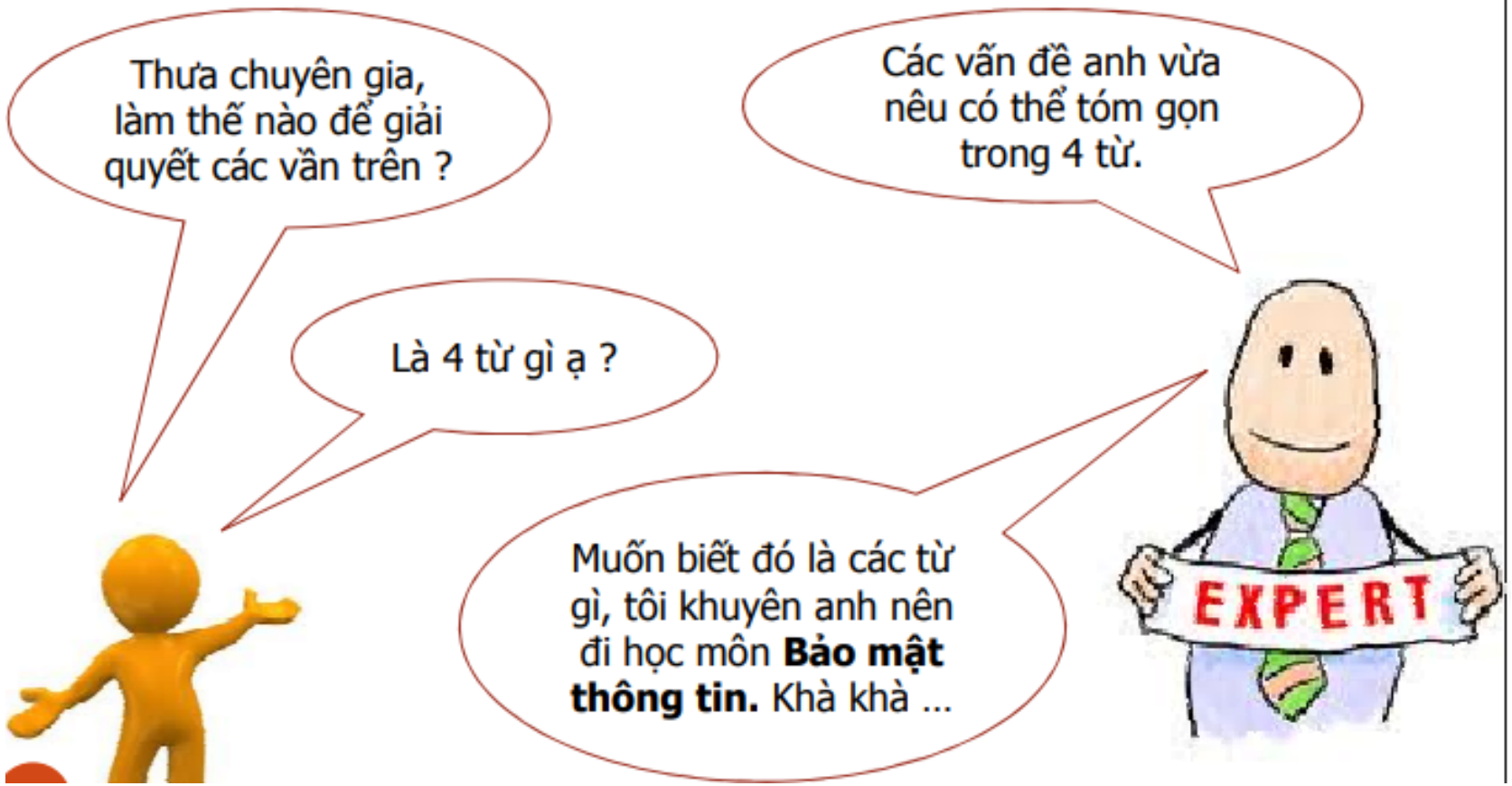
Tổng quan



6

1. Dẫn nhập tình huống

Tại sao phải học AT&BMTT ?



1. Dẫn nhập

- Về phạm vi: an ninh thông tin xét theo các mức cá nhân, tổ chức (doanh nghiệp) và quốc gia
- **"An ninh thông tin"** – trạng thái được bảo vệ của thông tin và vật mang tin (thuộc sở hữu cá nhân, tổ chức, hệ thống và các phương pháp bảo đảm sự tiếp nhận, xử lý, lưu trữ,lan truyền và sử dụng thông tin) trước các nguy cơ khác nhau
- Nguồn gốc các nguy cơ có thể biết trước (ăn cắp thông tin), có thể không biết trước (không rõ mục tiêu của tội phạm)

1. Dẫn nhập

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

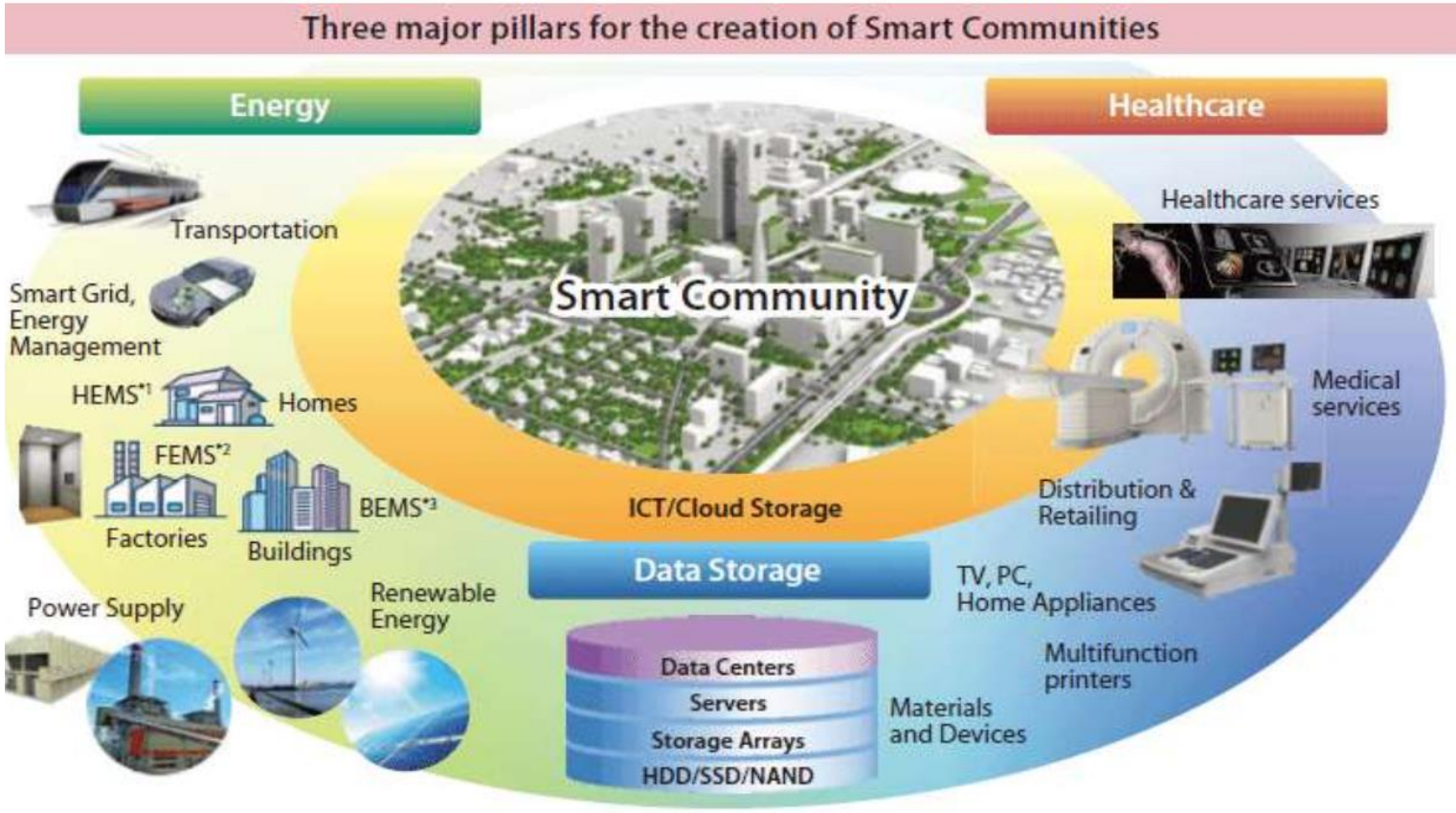
- Do chúng ta sống trong "thế giới kết nối" với mức độ ngày càng "sâu"
- Nhiều nguy cơ, đe dọa mất an toàn thông tin, an toàn dữ liệu

1. Dẫn nhập

Mọi thiết bị tính toán & truyền thông đều có kết nối Internet;

Các hệ thống kết nối "sâu và rộng" ngày càng phổ biến:

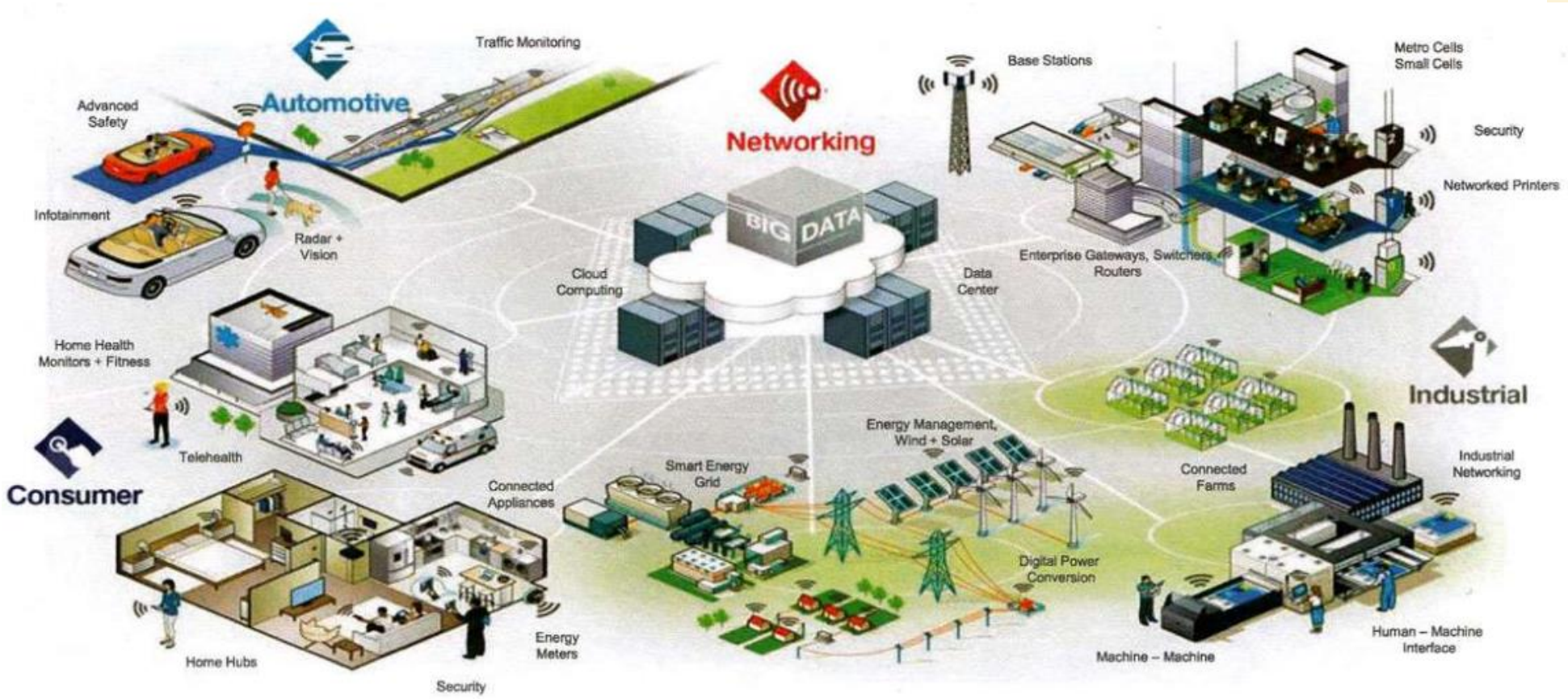
- ***Smart community*** *(cộng đồng thông minh)*
- ***Smart city*** *(thành phố thông minh)*
- ***Smart home*** *(ngôi nhà thông minh),…*



1. Dẫn nhập

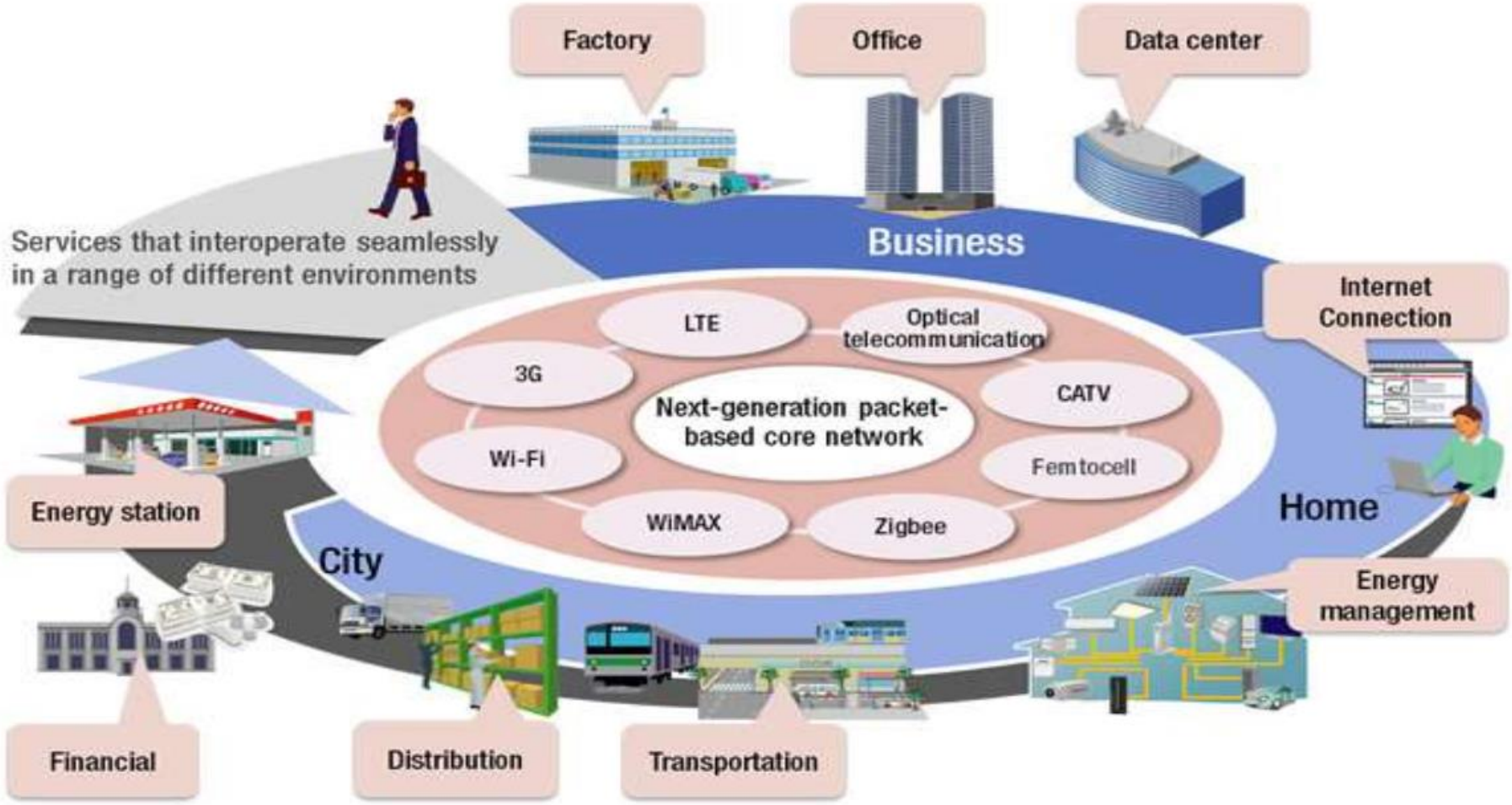
Các khái niệm kết nối mọi vật, kết nối tất cả trở nên "nóng":

- **IoT: Internet of Things**
- **IoE: Internet of Everything.**



1. Dẫn nhập

Các hệ thống không có kết nối khả năng sử dụng hạn chế.



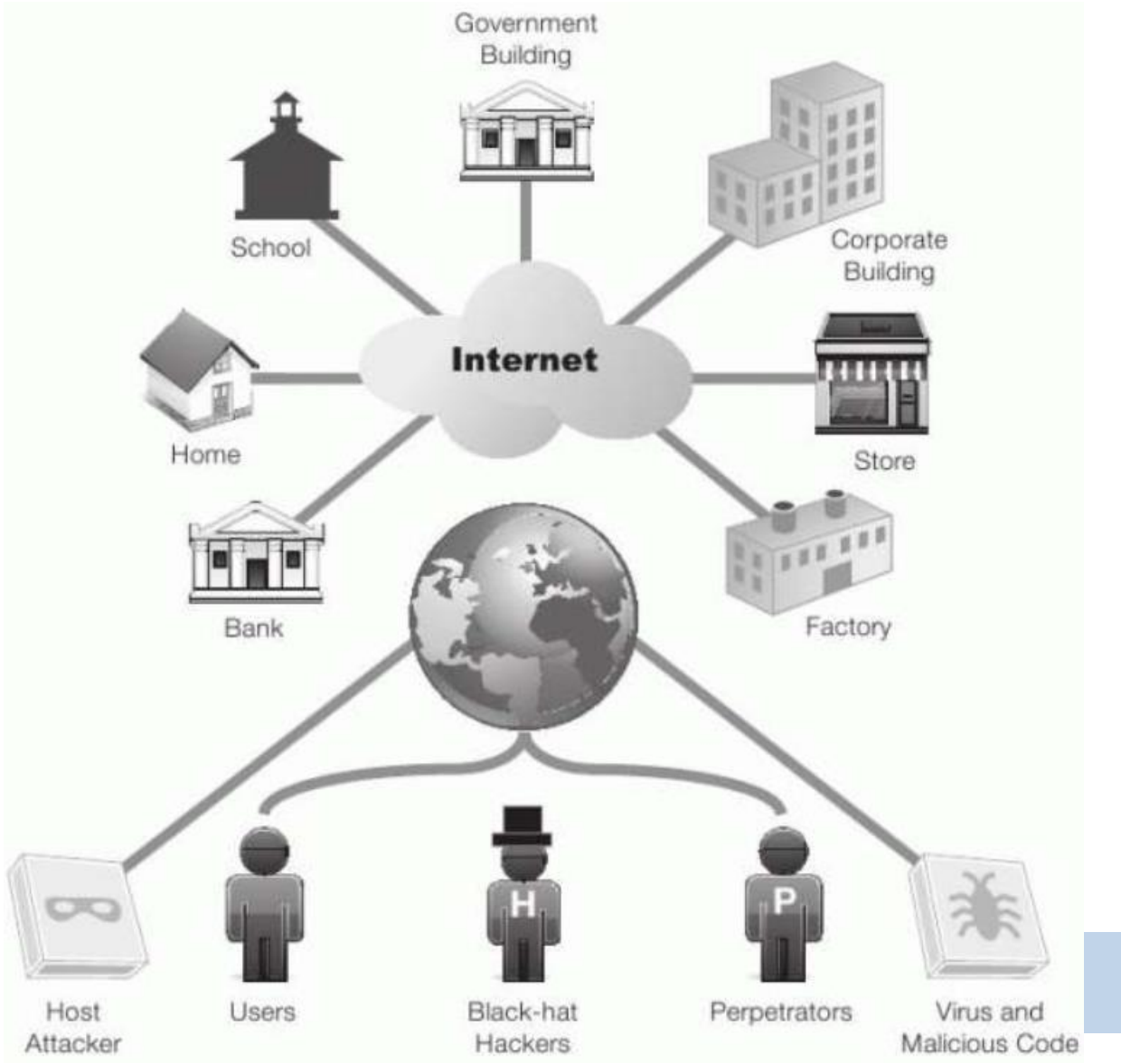
1. Dẫn nhập

Ngày càng có nhiều nguy cơ, đe dọa mất an toàn thông tin, trong hệ thống thông tin, trong mạng:

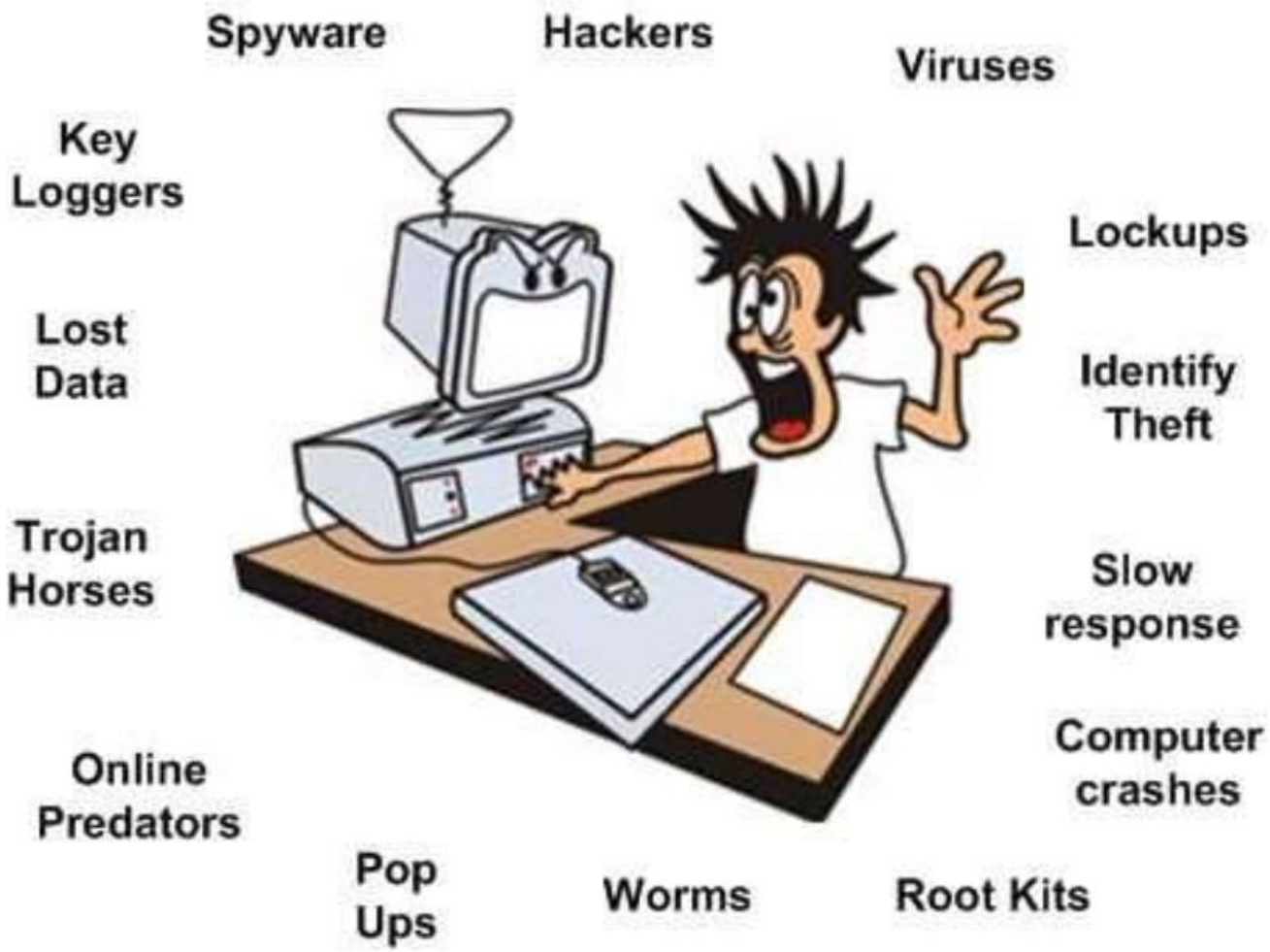
- Bị tấn công từ tin tặc
- Bị tấn công hoặc lạm dụng từ người dùng
- Lây nhiễm các phần mềm độc hại (vi rút, sâu,...)
- Nguy cơ bị nghe trộm, đánh cắp và sửa đổi thông tin
- Lỗi hoặc các khiếm khuyết phần cứng, phần mềm

1. Dẫn nhập

Thế giới kết nối
với nhiều
nguy cơ và đe dọa



1. Dẫn nhập



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

Mục đích bảo vệ thông tin

- Ngăn ngừa mất mát, gây nhiễu, tung tin …
- Ngăn ngừa đe dọa an ninh của cá nhân, xã hội, quốc gia
- Ngăn ngừa những hoạt động trái phép nhằm tiêu hủy, gây nhiễu, sao chép, gây tắc nghẽn thông tin; ngăn ngừa các dạng quấy rối vào tài nguyên thông tin và hệ thống thông tin
- Bảo vệ quyền công dân về sự riêng tư và tính bảo mật của dữ liệu cá nhân trong các hệ thống thông tin
- Bảo vệ bí mật quốc gia, tính bảo mật của thông tin văn bản tương ứng với quy định của luật pháp
- Bảo đảm quyền lợi của các chủ thể trong quá trình truyền thông, chế tác, sản xuất và sử dụng hệ thống thông tin

Biện pháp bảo vệ thông tin

- Hành chính
- Thiết bị kỹ thuật (phần cứng)
- Thuật toán (phần mềm)

➢ **Nhận xét:**

✓ Hiệu quả và kinh tế nhất: thuật toán

✓ Thực tế: kết hợp cả 3 biện pháp

An ninh thông tin

- **An ninh** – bảo đảm không thể gây hại đến hoạt động và thuộc tính của một đối tượng nào đó, kể cả cấu trúc và thành phần của nó
- An ninh của một đối tượng có thể phân chia thành nhiều dạng khác nhau.

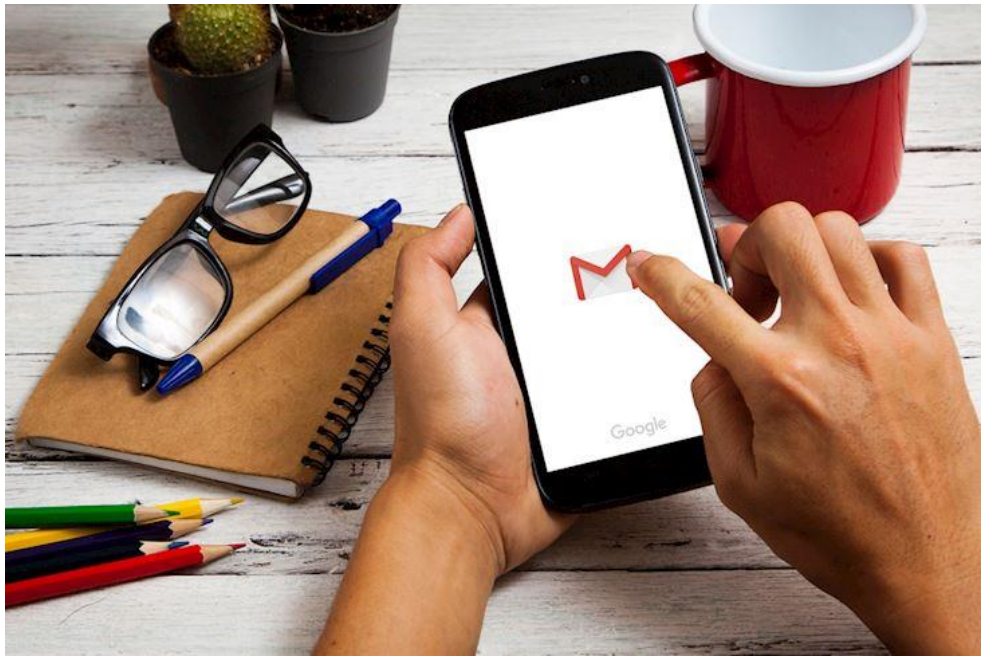
Một trong những dạng đó là **an ninh thông tin** (bảo vệ thông tin và những hoạt động với thông tin)

Vai trò An ninh thông tin

- Thông tin đối với con người cũng rất cần thiết như không khí, thức ăn, nước uống.
- Thông tin giúp con người nâng cao hiệu quả công việc, phát sinh nhu cầu xã hội, phát triển cá tính, tự tin …
- Thông tin là phương tiện cơ bản trong giao tiếp, thiếu phương tiện này đa phần các nhiệm vụ không thể hoàn thành
- Thông tin giúp tồn tại quá trình đào tạo, giáo dục để truyền đạt kiến thức, kinh nghiệm …
- Gây tổn hại đến thông tin hay khả năng tiếp nhận, suy nghĩ của một người chính là làm giảm sức sống của người đó
- An ninh thông tin cá nhân là đảm bảo an toàn thông tin riêng tư, hoạt động xã hội dựa trên cơ sở suy luận, suy nghĩ từ thông tin nhận được

Vai trò thông tin với cá nhân

- Nhằm nâng cao hiệu quả hoạt động với thông tin, con người dùng các thiết bị hỗ trợ:



Vai trò thông tin với Doanh nghiệp

- Mỗi doanh nghiệp, tổ chức được xem là một hệ thống (sự liên kết nhân lực, vật lực để tiến đến mục đích chung)

- **Thông tin**

Dữ liệu → thông tin → tri thức

- **An toàn**

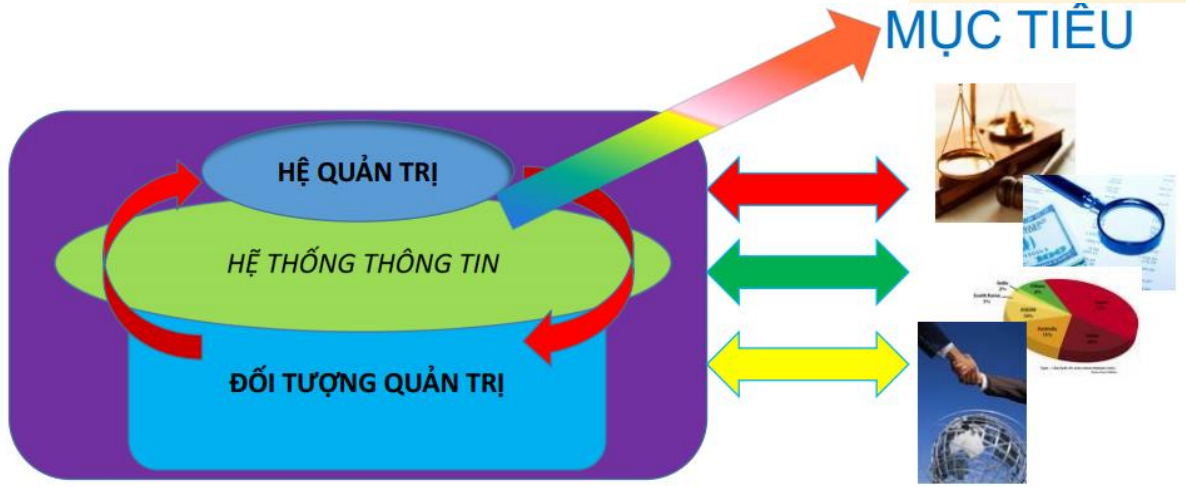
Nguy cơ: tiết lộ thông tin, phát thông tin sai, phá hoại, chiếm quyền điều khiển

Biện pháp: Ngăn chặn, phát hiện, phục hồi

- **An toàn thông tin**

CIA: Bảo mật, toàn vẹn, khả dụng

Mở rộng: Tiện ích, xác thực, sở hữu



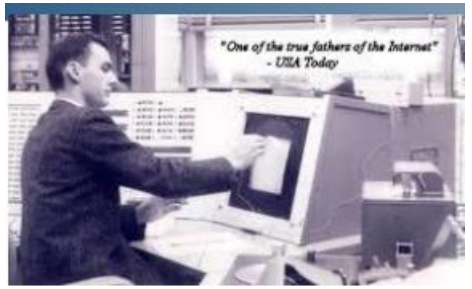
2. Lịch sử:

- **1930s**

Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or *Unterseeboot* version of the Enigma, caused considerable anguish to Allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. "Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it."[1]

1960s

- Chiến tranh lạnh
- Larry Roberts
- ARPANET(Mạng lưới cơ quan với các đề án nghiên cứu tân tiến).



DARPA

2. Lịch sử:

- **1970s – 1980s**

Date	Documents
1968	Maurice Wilkes discusses password security in *Time-Sharing Computer Systems.*
1973	Schell, Downey, and Popek examine the need for additional security in military systems in *"Preliminary Notes on the Design of Secure Military Computer Systems."*[5]
1975	The Federal Information Processing Standards (FIPS) examines Digital Encryption Standard (DES) in the *Federal Register.*
1978	Bisbey and Hollingworth publish their study "Protection Analysis: Final Report," discussing the Protection Analysis project created by ARPA to better understand the vulnerabilities of operating system security and examine the possibility of automated vulnerability detection techniques in existing system software.[6]
1979	Morris and Thompson author "Password Security: A Case History," published in the Communications of the Association for *Computing Machinery* (ACM). The paper examines the history of a design for a password security scheme on a remotely accessed, time-sharing system.
1979	Dennis Ritchie publishes "On the Security of UNIX" and "Protection of Data File Contents," discussing secure user IDs and secure group IDs, and the problems inherent in the systems.
1984	Grampp and Morris write "UNIX Operating System Security." In this report, the authors examine four "important handles to computer security": physical control of premises and computer facilities, management commitment to security objectives, education of employees, and administrative procedures aimed at increased security.[7]
1984	Reeds and Weinberger publish "File Security and the UNIX System Crypt Command." Their premise was: "No technique can be secure against wiretapping or its equivalent on the computer. Therefore no technique can be secure against the systems administrator or other privileged users ... the naive user has no chance."[8]

2. Lịch sử:

- **1990s**
  - Mạng máy tính → Phổ biến
    - Mạng internet: 1990s
    - Người dùng internet & email:

      Computer scientist (Khoa học máy tính).

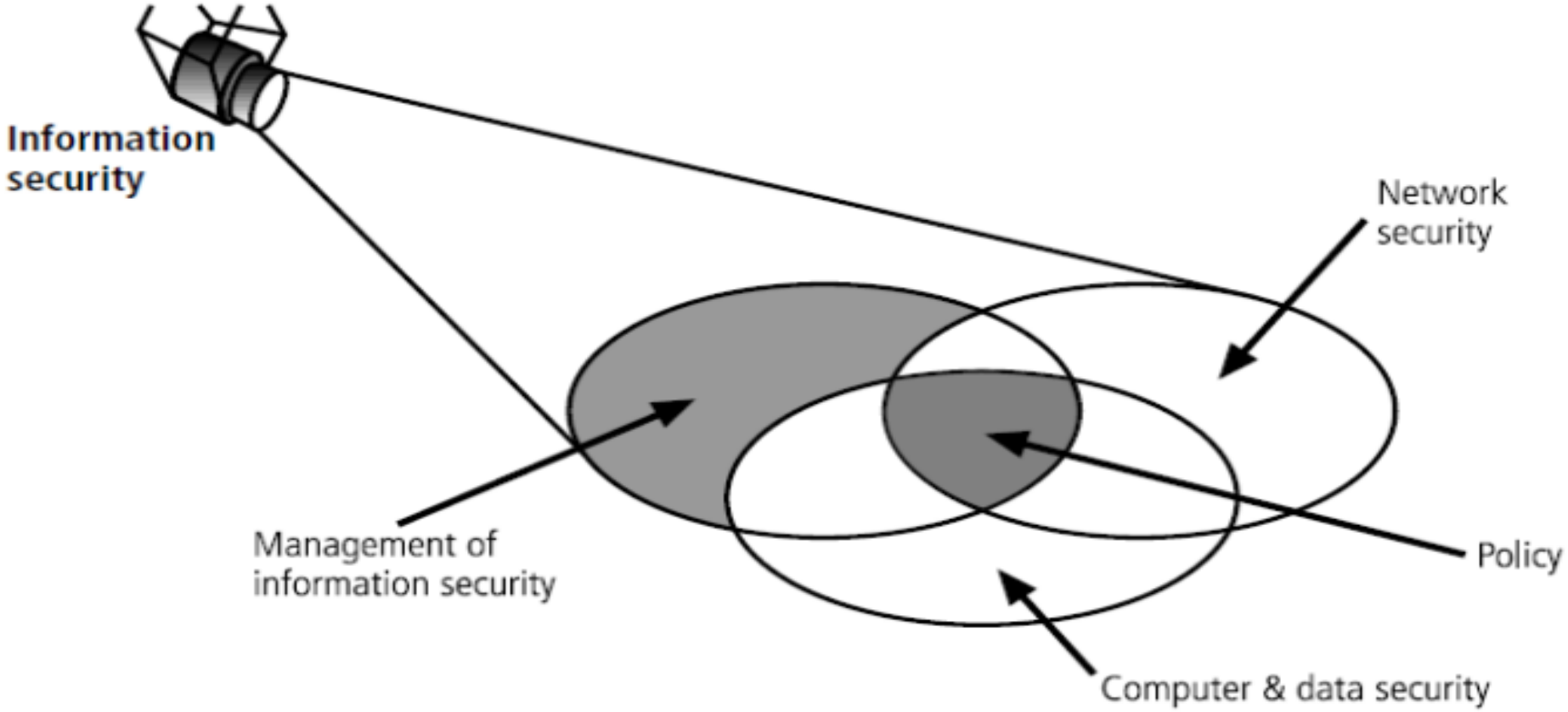
→ mail server authentication and e-mail encryption did not seem necessary

2. Lịch sử:

- **2000 to Present**

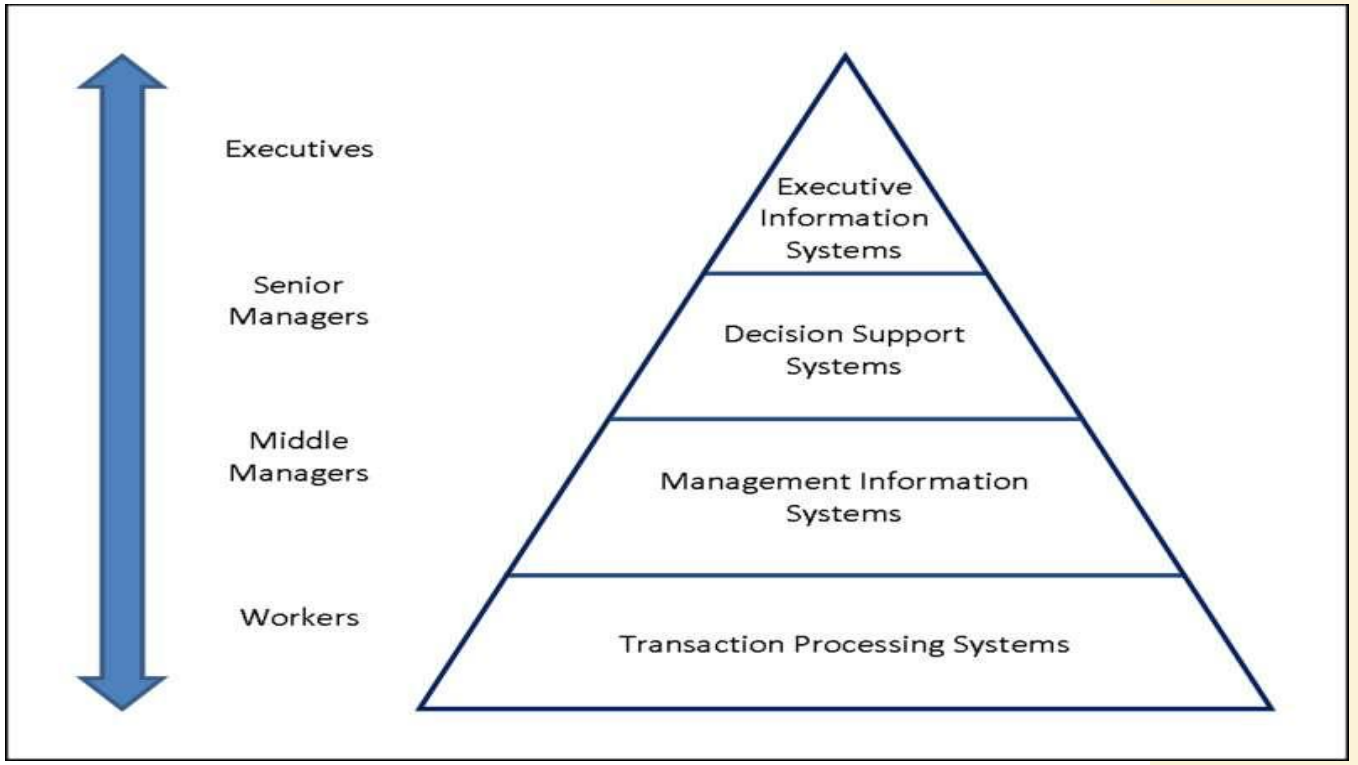
3. Bảo mật thông tin là gì?

là bảo vệ thông tin dữ liệu cá nhân, tổ chức nhằm tránh khỏi sự " đánh cắp, ăn cắp" bởi những kẻ xấu hoặc tin tặc



Các đặc điểm thông tin

- Availability (Sẵn sàng)
- Accuracy (chính xác)
- Authenticity (xác thực)
- Confidentiality (bí mật)
- Integrity (toàn vẹn)
- Utility (tiện ích)
- Possession (khả dụng)



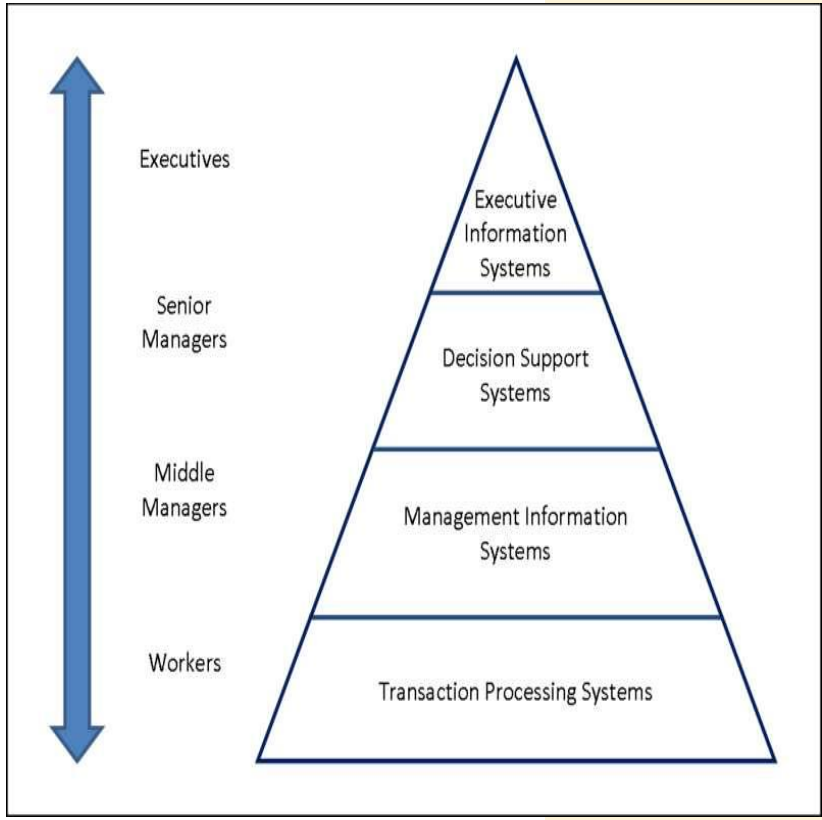
Hệ thống thông tin điều hành - giám đốc điều hành
Hệ thống hỗ trợ ra quyết định - quản lý cấp cao
Hệ thống thông tin quản lý - quản lý cấp trung
Hệ thống xử lý giao dịch - Người lao động

Các loại hệ thống thông tin (mô hình tháp)

Các đặc điểm thông tin

Các loại hệ thống thông tin (mô hình tháp)- gồm 4 loại theo đối tượng sử dụng:

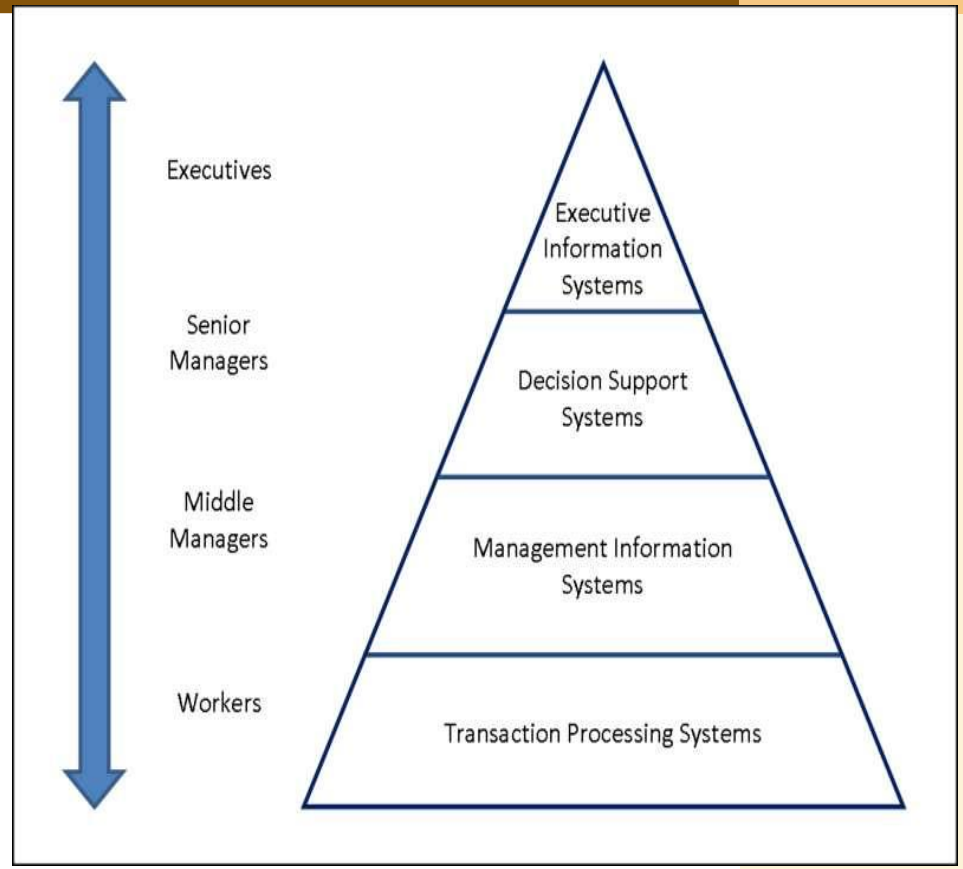
- *Hệ thống xử lý giao dịch (Transactional Processing Systems)* với người sử dụng là các nhân viên (Workers);
- *Hệ thống thông tin quản lý (Management Information Systems)* với người sử dụng là các quản lý bộ phận (Middle Managers);



Các loại hệ thống thông tin (mô hình tháp)

Các đặc điểm thông tin

- *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).



Các loại hệ thống thông tin (mô hình tháp)

Các đặc điểm 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).

Các đặc điểm 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

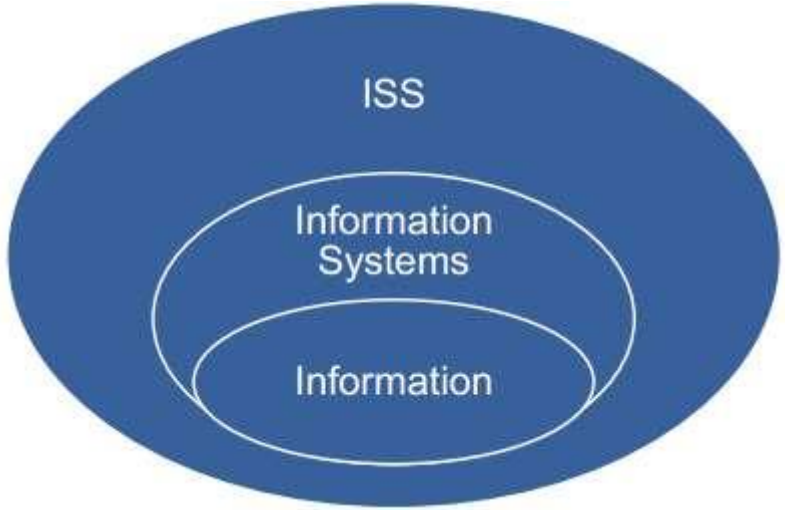
✓ Networks: hệ thống truyền dẫn thông tin/dữ liệu

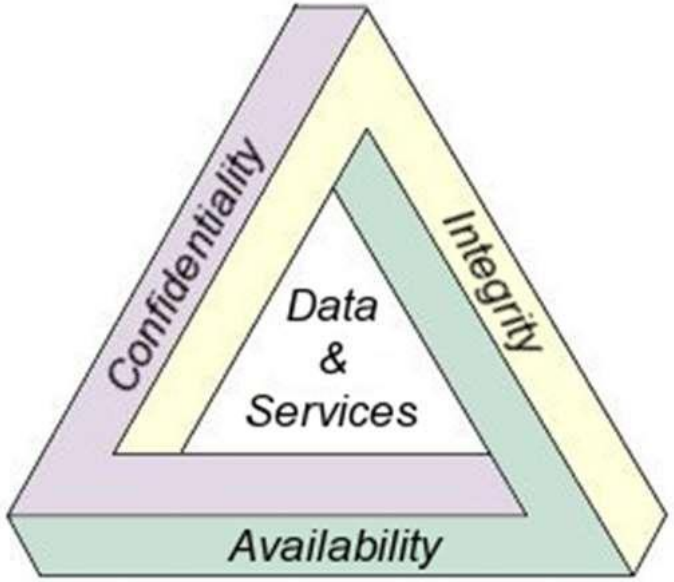
✓ Procedures: tập hợp các lệnh kết hợp các bộ phận nêu trên để xử lý dữ liệu, đưa ra kết quả mong muốn.

Các khái niệm bảo mật

An toàn thông tin (Information Security) là gì?

- An toàn thông tin là việc bảo vệ chống truy nhập (access), sử dụng (use), tiết lộ (disclose), sửa đổi (modify), hoặc phá hủy (destroy) thông tin một cách trái phép (unauthorised).





Các khái niệm bảo mật

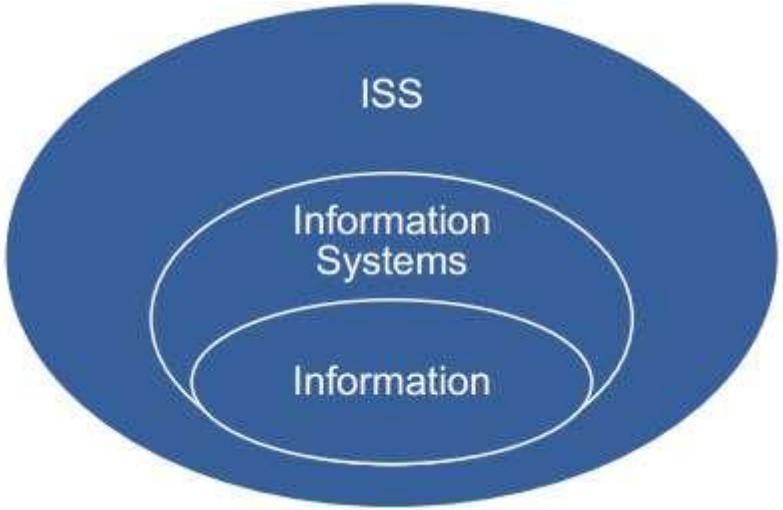
Hai lĩnh vực chính của an toàn thông tin (ATTT):

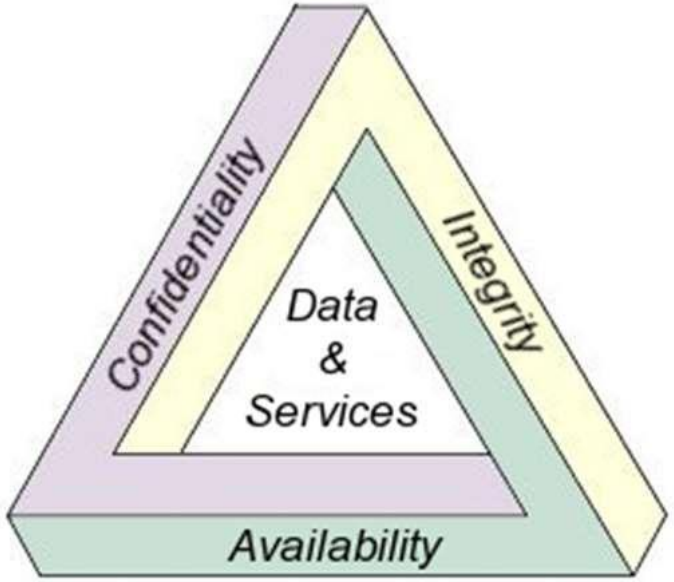
- **An toàn công nghệ thông tin (IT Security):**
  - Đôi khi còn gọi là an toàn máy tính (Computer Security) là ATTT áp dụng cho các hệ thống công nghệ;
  - Các hệ thống công nghệ thông tin của 1 tổ chức cần được đảm bảo an toàn khỏi các tấn công mạng.
- **Đảm bảo thông tin (Information Assurance):**
  - 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)

Các khái niệm bảo mật

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, bao gồm:

- Bí mật (**Confidentiality**)
- Toàn vẹn (**Integrity**)
- Sẵn dùng (**Availability**)



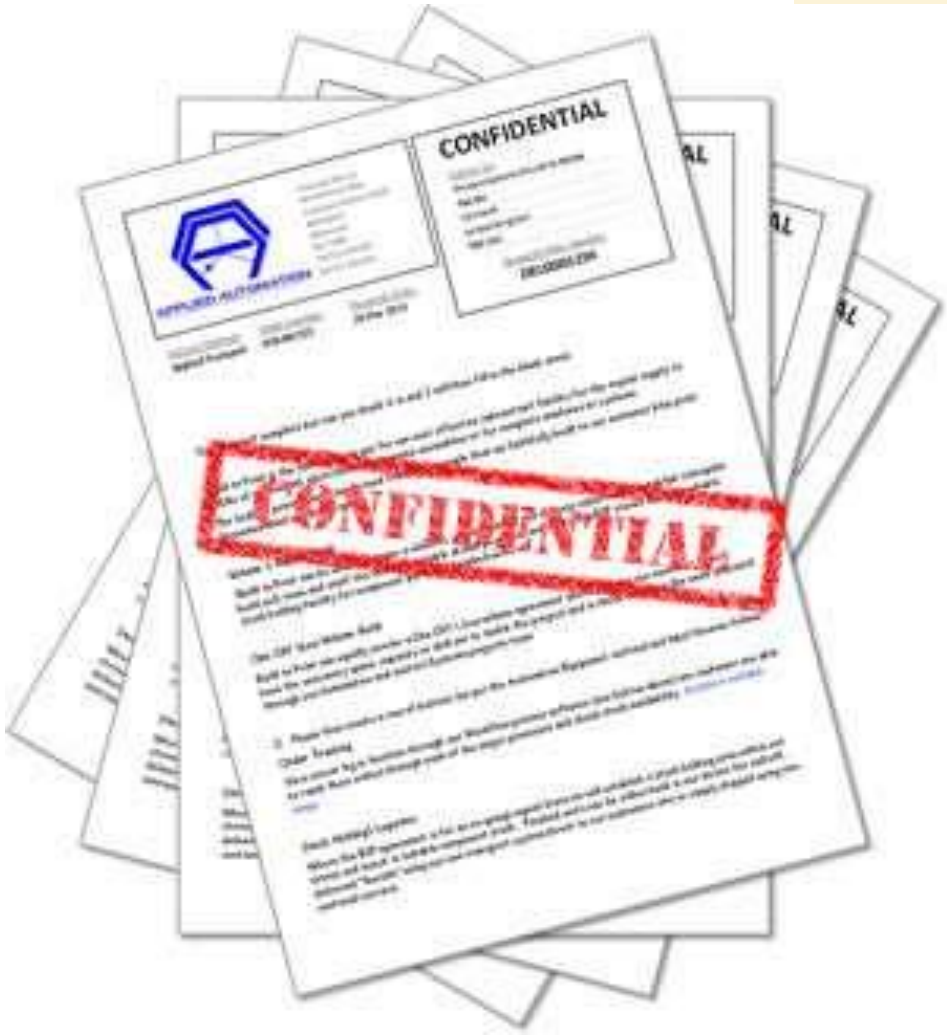


Các khái niệm bảo mật

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



Các khái niệm bảo mật

Tính toàn vẹn (Integrity):

thông tin chỉ có thể được sửa đổi bởi những người dùng có thẩm quyền.

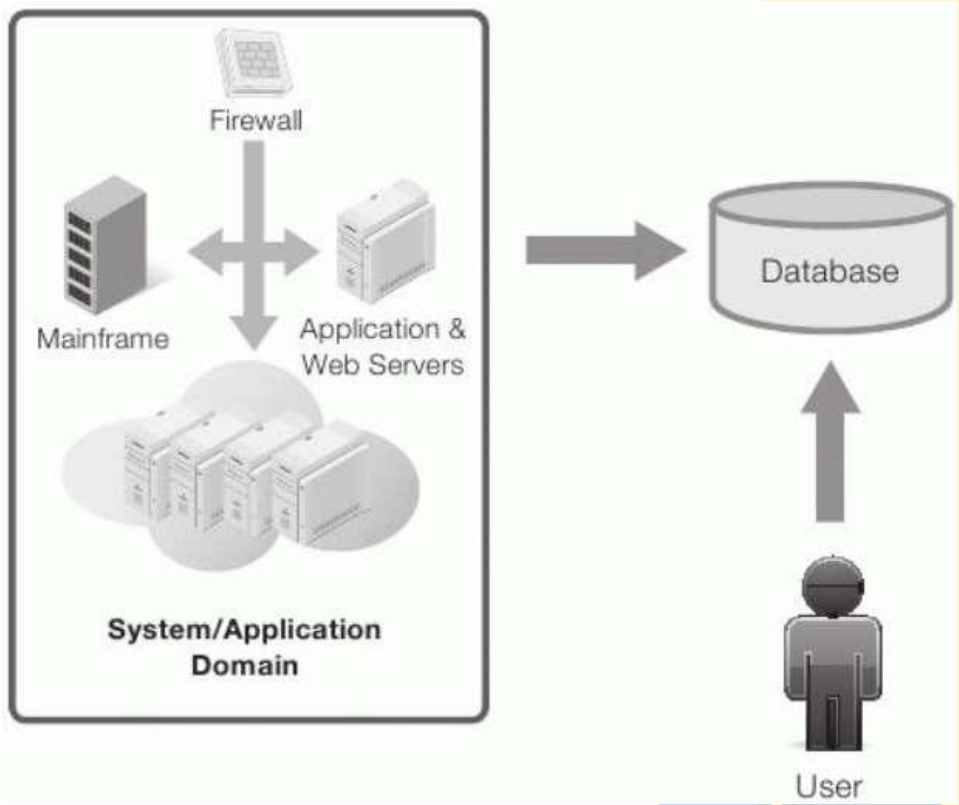
❖Tính toàn vẹn liên quan đến tính hợp lệ validity) và chính xác (accuracy) của dữ liệu.

- 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.

Thông tin chỉ có thể được sửa đổi bởi người dung có thẩm quyền.



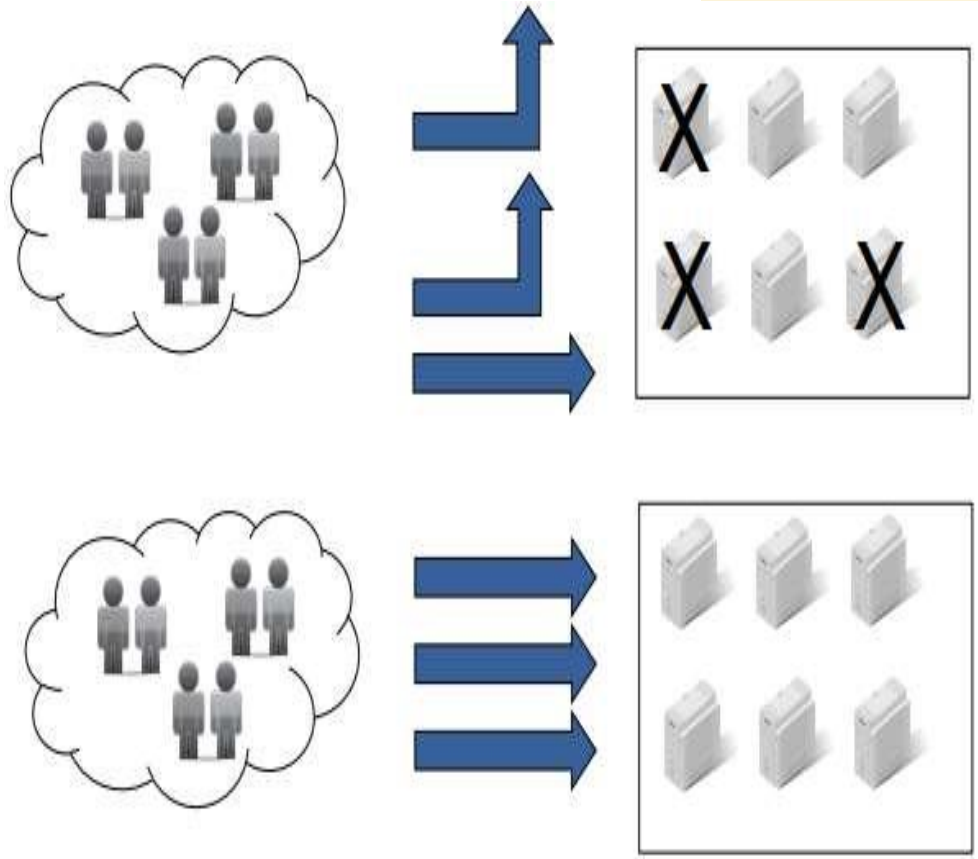
Các khái niệm bảo mật

Tính sẵn dùng (Availability):

thông tin có thể truy nhập bởi người dùng hợp pháp bất cứ khi nào họ có yêu cầu.

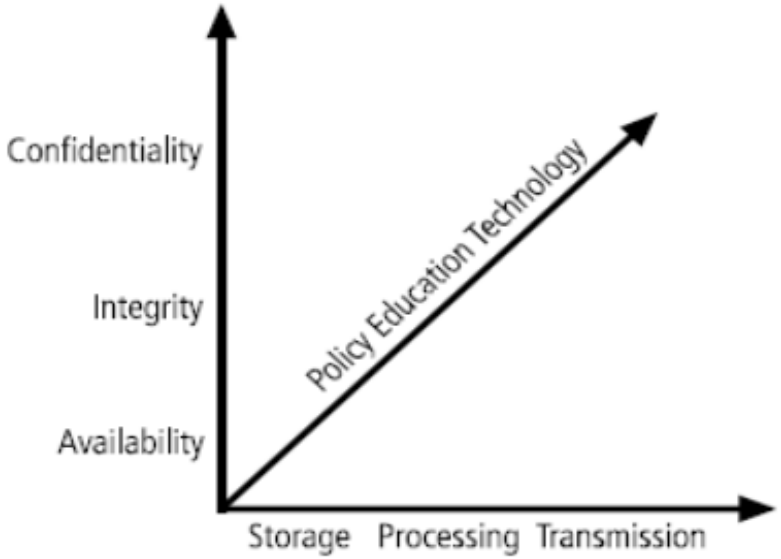
❖Tính sẵn dùng có thể được đo bằng các yếu tố:

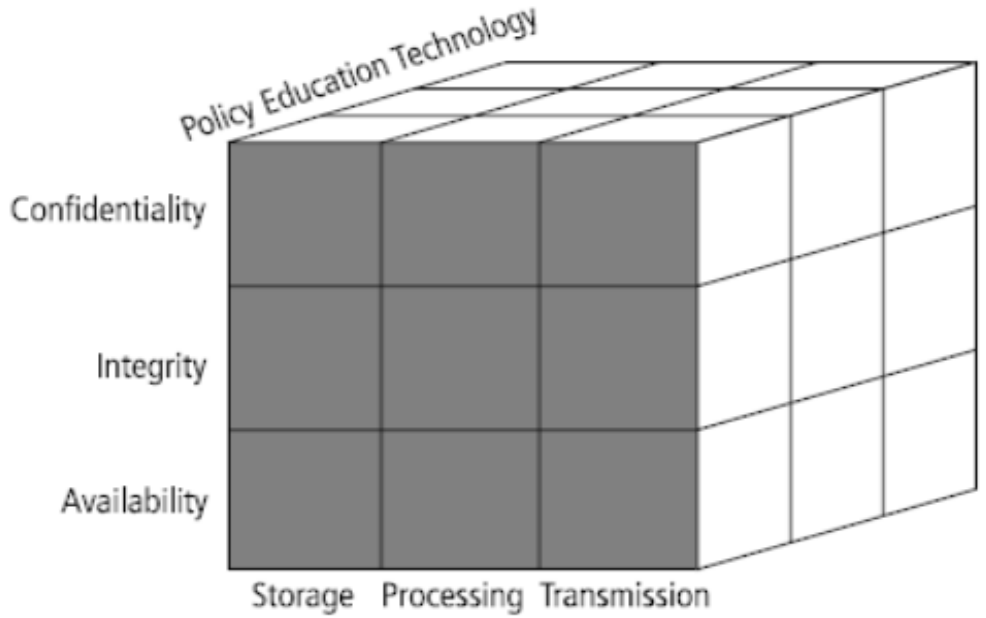
- Thời gian cung cấp dịch vụ (Uptime);
- Thời gian ngừng cung cấp dịch vụ (Downtime);
- Tỷ lệ phục vụ: A = (Uptime)/(Uptime + Downtime);
- Thời gian trung bình giữa các sự cố;
- Thời gian trung bình ngừng để sửa chữa;
- Thời gian khôi phục sau sự cố.



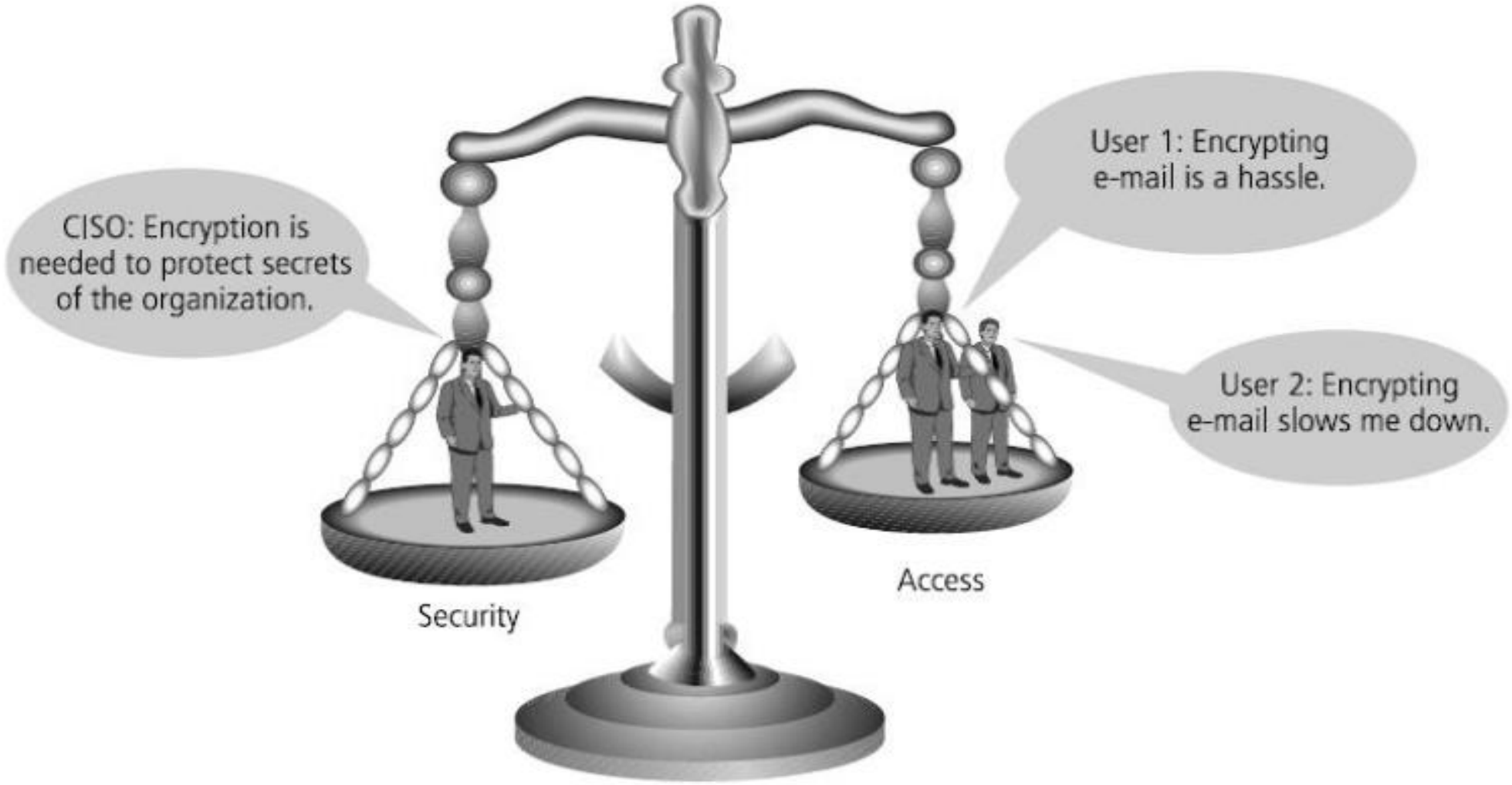
Định nghĩa Bảo mật

Cần phải tuân thủ các tiêu chuẩn của Liên minh Viện thông Quốc tế (ITU): "***Bảo mật mạng là tập hợp các công cụ, chính sách, khái niệm về bảo mật, hướng dẫn , phương pháp quản lý rủi ro, phản ứng, đào tạo, diễn tập, thiết bị và công nghệ có thể được dùng để bảo vệ hệ thống mạng và tài sản.*** "

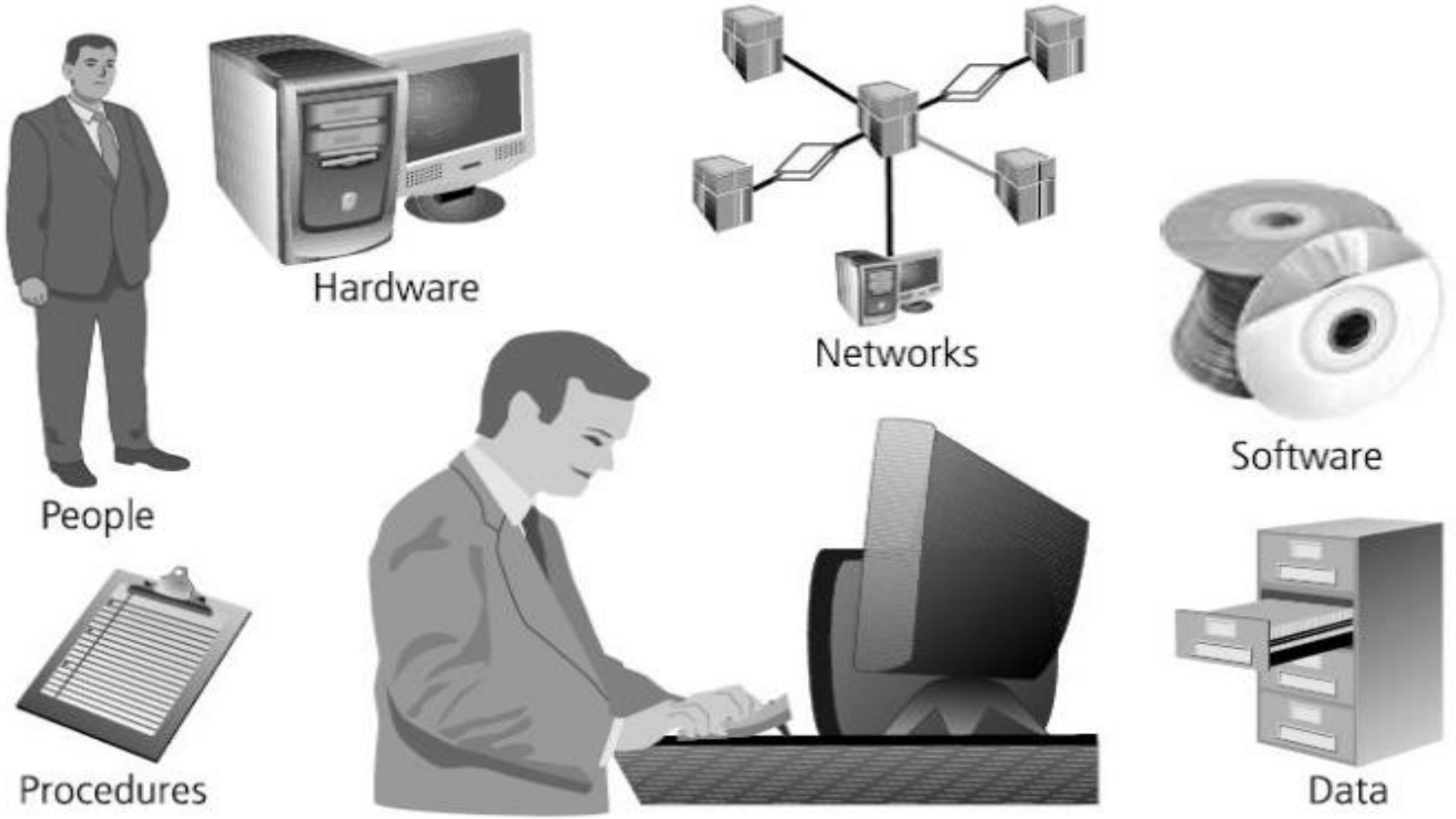




Bảo mật và quyền truy cập



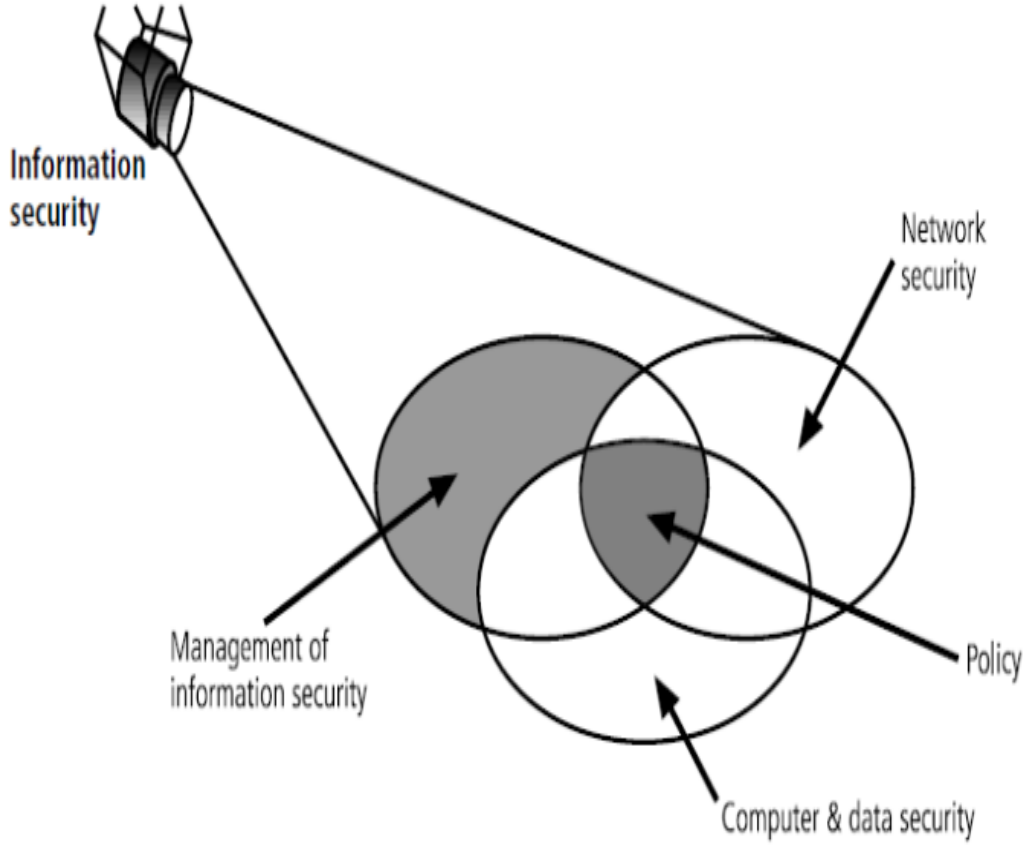
4. Các thành phần HTTT



4. Các thành phần HTTT

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)



4. Các thành phần HTTT

An toàn máy tính và dữ liệu:

- ✓ Đảm bảo an toàn hệ điều hành, ứng dụng, dịch vụ;
- ✓ Vấn đề điều khiển truy nhập;
- ✓ Vấn đề mã hóa và bảo mật dữ liệu;
- ✓ Vấn đề phòng chống phần mềm độc hại;
- ✓ Việc sao lưu tạo dự phòng dữ liệu, đảm bảo dữ liệu lưu trong máy tính không bị mất mát khi xảy ra sự cố.

4. Các thành phần HTTT

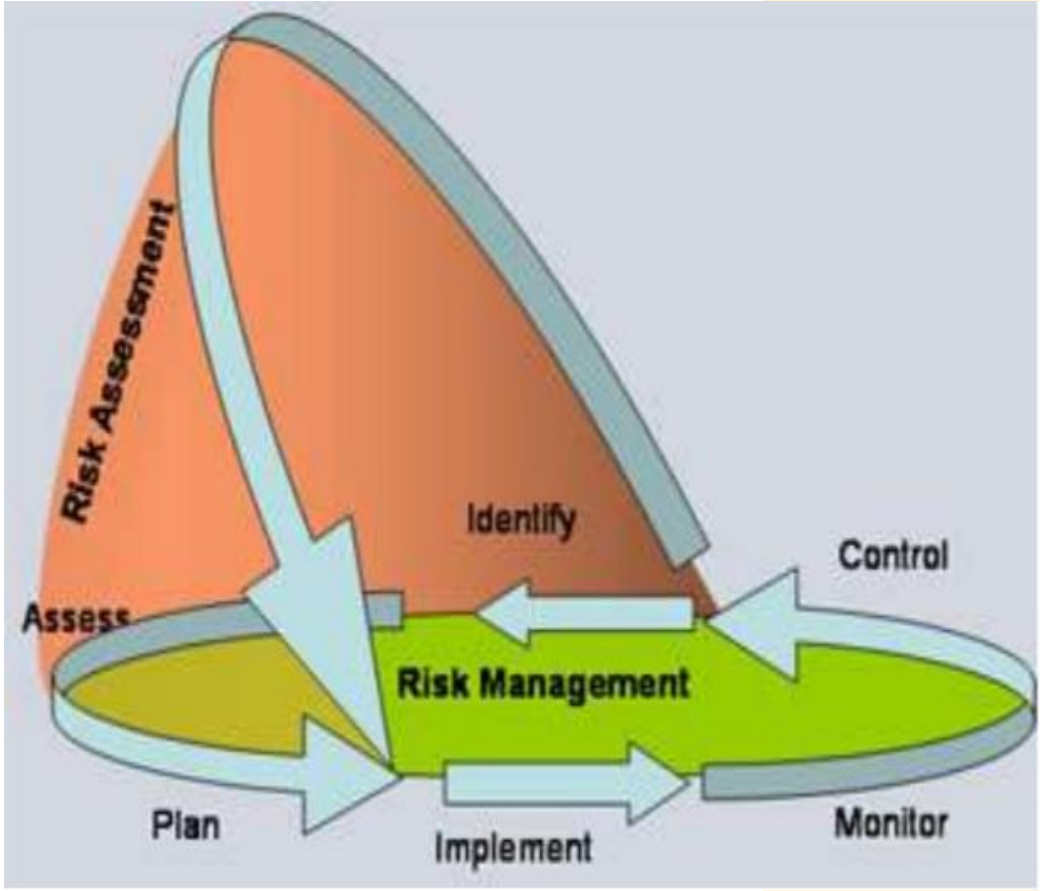
An ninh mạng:

- ✓ Các tường lửa, proxy cho lọc gói tin và điều khiển truy nhập;
- ✓ Mạng riêng ảo và các kỹ thuật bảo mật thông tin truyền như SSL/TLS, PGP;
- ✓ Các kỹ thuật và hệ thống phát hiện, ngăn chặn tấn công, xâm nhập;
- ✓ Vấn đề giám sát mạng.

4. Các thành phần HTTT

Quản lý an toàn thông tin:

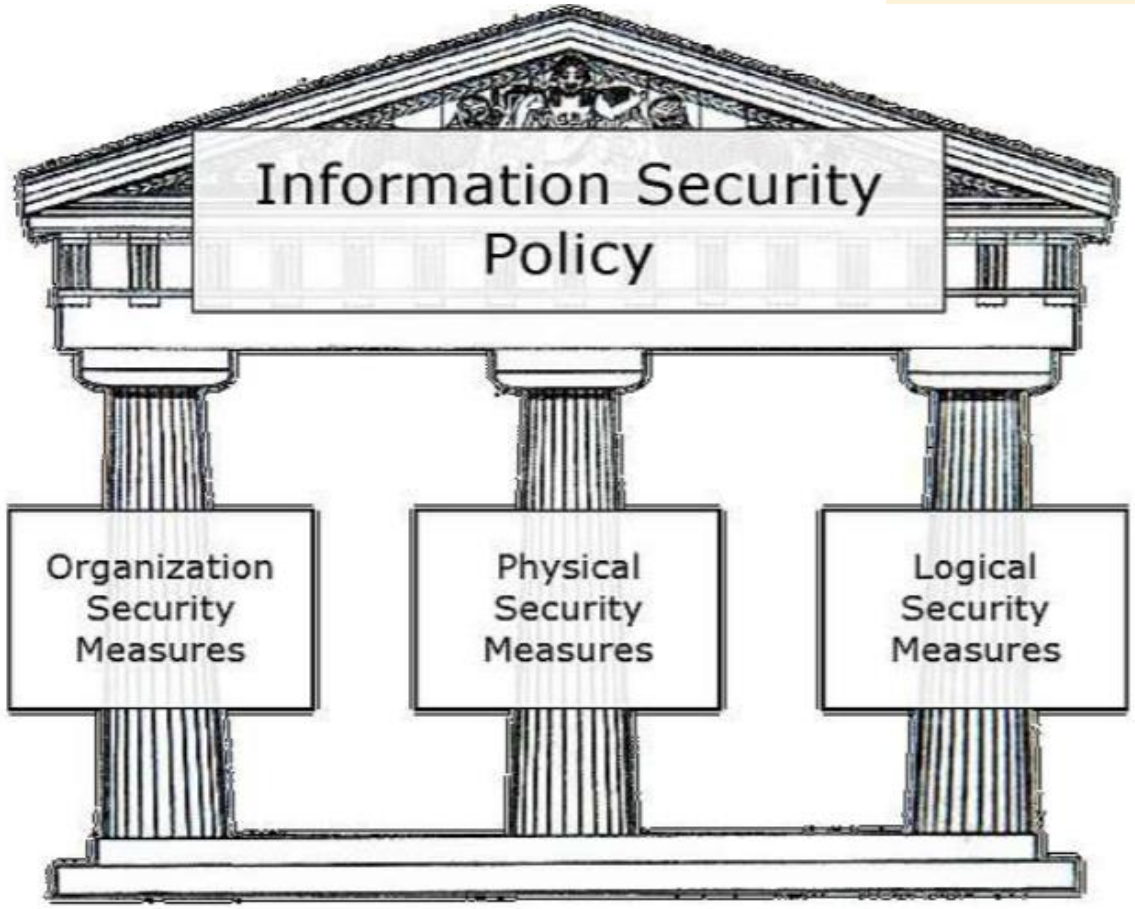
- ❖ **Quản lý rủi ro**
  - ✓ Nhận dạng
  - ✓ Đánh giá
- ❖ **Thực thi quản lý an toàn thông tin**
  - ✓ Lập kế hoạch (Plan)
  - ✓ Thực thi kế hoạch (Do/Implement)
  - ✓ Giám sát kết quả thực hiện (Monitor)
  - ✓ Thực hiện các kiểm soát (Control).



4. Các thành phần HTTT

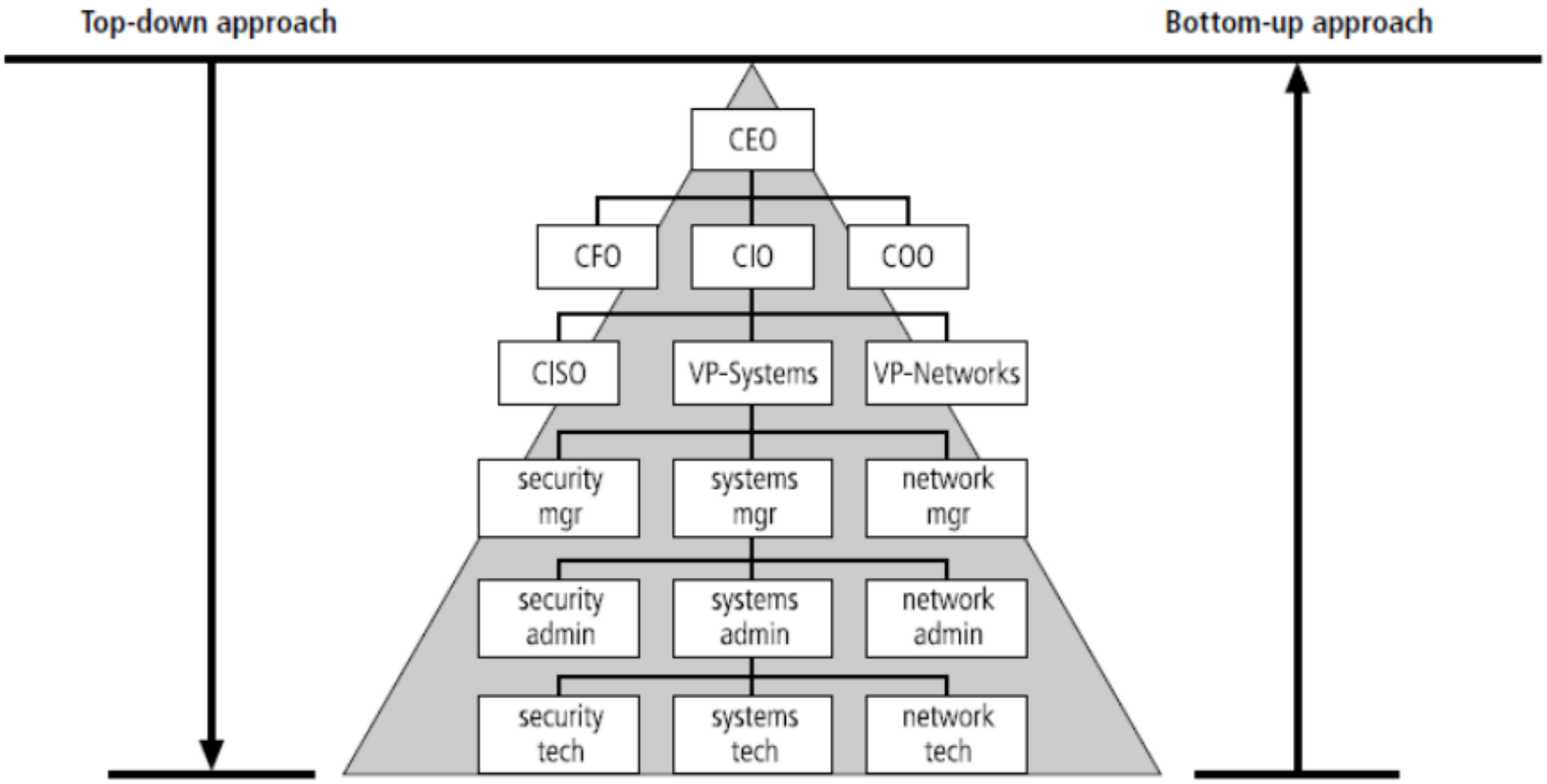
Chính sách an toàn thông tin:

- ✓ Chính sách an toàn ở mức vật lý (Physical security policy)
- ✓ Chính sách an toàn ở mức tổ chức (Organizational security policy)
- ✓ Chính sách an toàn ở mức logic (Logical security policy).



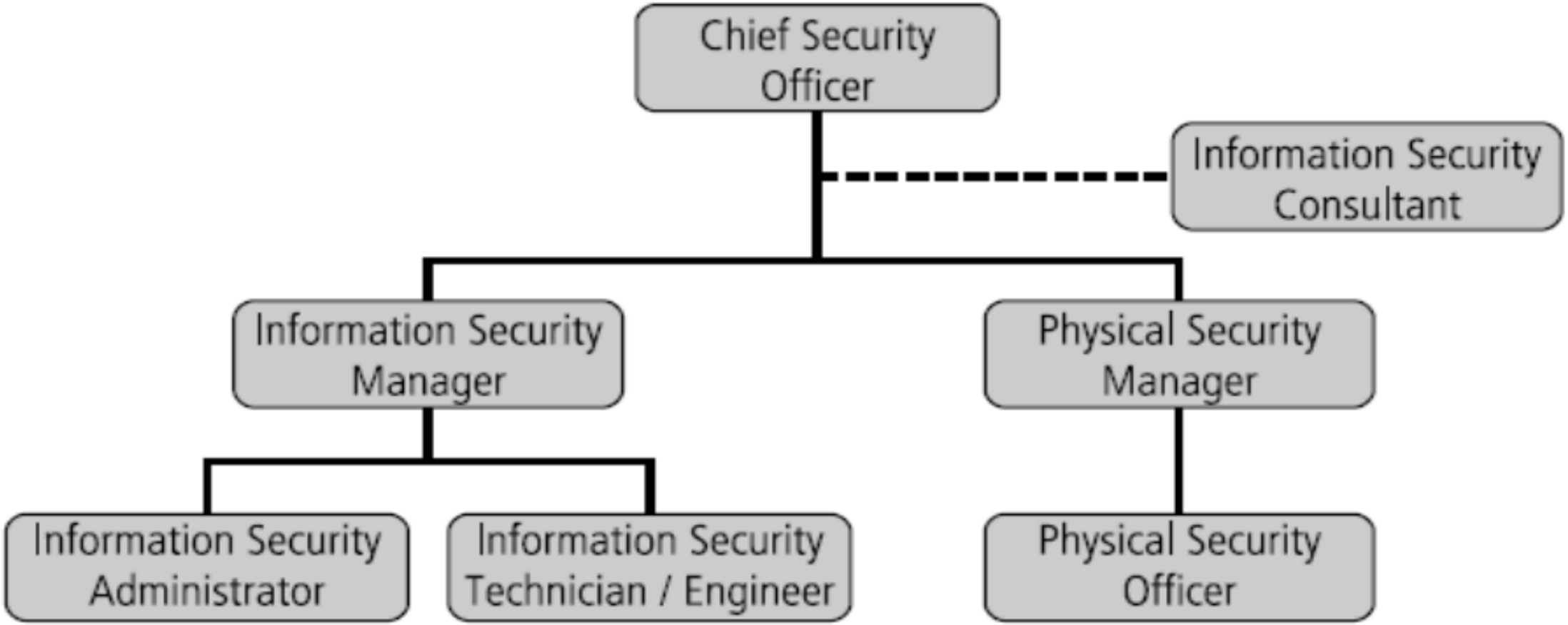
5. Tiếp cận phương pháp bảo mật thông tin

Mô hình quản lý thông tin doanh nghiệp



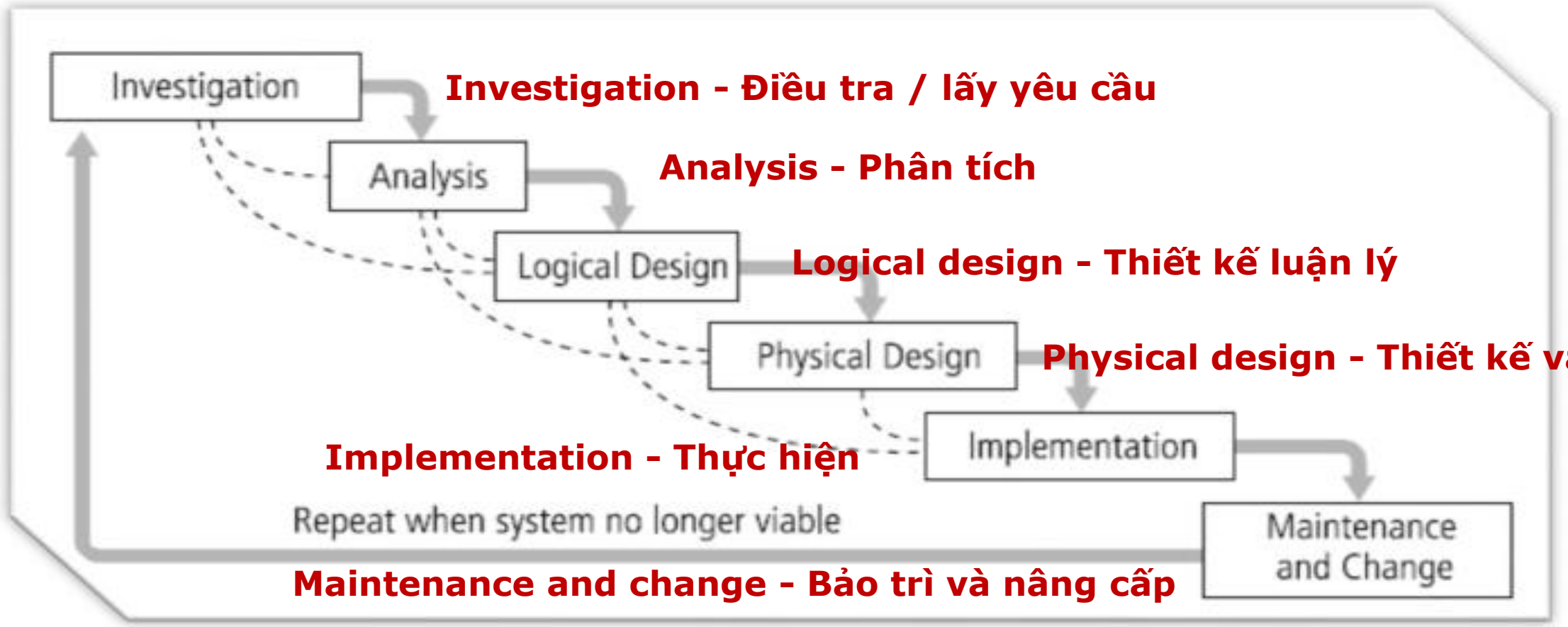
5. Tiếp cận phương pháp bảo mật thông tin

Vị trí ATTT trong doanh nghiệp



5. Tiếp cận phương pháp bảo mật thông tin

Vòng đời phát triển hệ thống



Investigation - Điều tra / lấy yêu cầu

Analysis - Phân tích

Logical design - Thiết kế luận lý

Physical design - Thiết kế vật lý

Implementation - Thực hiện

Maintenance and change - Bảo trì và nâng cấp

5. Tiếp cận phương pháp bảo mật thông tin

1. Investigation - Điều tra / lấy yêu cầu

- Phác thảo phạm vi và mục tiêu dự án
- Ước tính chi phí
- Đánh giá nguồn lực hiện có
- phân tích tính khả thi

2. Analysis - Phân tích

- Đánh giá hệ thống hiện tại so với kế hoạch phát triển trong giai đoạn 1
- Phát triển sơ bộ yêu cầu hệ thống
- Nghiên cứu tích hợp hệ thống mới với hệ thống hiện có
- Tìm kiếm tài liệu và cập nhật phân tích khả thi

5. Tiếp cận phương pháp bảo mật thông tin

3. Logical design - Thiết kế luận lý

- Đánh giá nhu cầu kinh doanh hiện tại so với kế hoạch phát triển trong giai đoạn 2
- Lựa chọn ứng dụng, dữ liệu và mô hình
- Tạo ra nhiều giải pháp để xem xét
- Tìm kiếm tài liệu và cập nhật phân tích khả thi

4. Physical design - Thiết kế vật lý

- Lựa chọn công nghệ hỗ trợ cho giải pháp được phát triển trong giai đoạn 3
- Lựa chọn giải pháp tối ưu nhất
- Quyết định tự làm hoặc mua các phần liên quan
- Tìm kiếm tài liệu và cập nhật phân tích khả thi

5. Tiếp cận phương pháp bảo mật thông tin

5. Implementation - Thực hiện

- Tự phát triển hoặc mua phần mềm
- Đặt hàng các component
- Document the system
- Train users
- Cập nhật phân tích khả thi
- Present system to users
- Test system and review performance

6. Maintenance and change - Bảo trì và nâng cấp

- Hỗ trợ và chỉnh sửa hệ thống trong suốt thời gian hoạt động
- Kiểm tra định kỳ cho phù hợp với kinh doanh
- Nâng cấp và vá lỗi khi cần thiết

TÓM TẮT CHƯƠNG VÀ BÀI TẬP

TÓM TẮT:

Định nghĩa bảo mật
Các thành phần HTTT
Tiếp cận phương pháp bảo mật thông tin

BÀI TẬP:

Chuẩn bị thuyết trình nhóm tối đa 2 bạn.
Chương 2: Các mối đe doạ và tấn công mạng
- Trình bày các lỗ hổng mạng máy tính có thể gặp phải?
- Ví dụ minh họa trong thực tế đã gặp.
- Phân tích cách thức khai thác tấn công các lỗ hổng mạng
- Phương pháp phòng chống

Thanks.